INFORMATION ASSURANCE AND CYBER SECURITY STRATEGIC PLAN

CONTENTS

FIGURES

TABLES

1 EXECUTIVE SUMMARY

1 EXECUTIVE SUMMARY

In 2010, the Office of the Governor introduced a New Day Plan designed to take a fresh look at many of State's most significant investments with the aim of enhancing efficiency and effectiveness in key areas. The Information Technology (IT) program was an investment focused on early in the new administration. The State's IT program supports a complex, diverse, and multifaceted mission and has been identified as requiring enhancements to its IT security component. In recognition of the need to provide these enhancements, the State's IT management has undertaken efforts to address IT security and compliance areas that need enhancement to provide the additional protection to sensitive State and personal information by refocusing its resources and reevaluating its goals. The result of this re-evaluation is reflected in the following plans: Information Assurance and Cyber Security Program Management, the Information Assurance and Cyber Security Strategic, Information Assurance and Cyber Security Governance, Disaster Recovery and Continuity of Government, and Privacy.

This document presents State's Information Assurance and Cyber Security Strategic Plan supporting this initiative. Strategic plans covering all aspects of business, IT, and information resource management (IRM) have also been developed and identified as Phase II transformation efforts. Although the projects and the strategy have been well vetted, they are subject to change pending final approval of State's IT Governance Plan.

The Information Assurance and Cyber Security Strategic Plan, referred to as the Plan, has been prepared in response to the Chief Information Officer Council (CIOC), Enterprise Leadership Council (ELC), and the Enterprise Architecture Advisory Working Group (EA-AWG) as a vital component of the State of Hawai`i Business and IT/IRM Strategic Transformation Plan. The Plan is a direct result of briefings provided to the Chief Information Officer (CIO) addressing improvement of the Information Resources Management of information assurance and cyber security within the State. Under the leadership of the CIO, the Information Assurance and Privacy Advisory Working Group (IA&P-AWG), hereafter referred to as the authors, prepared this document. This Plan recommends both a strategic and tactical approach to IT security improvements using a risk management framework that addresses current and future needs of the State's security posture while recognizing the technical, financial, and cultural needs of State's organizational subcomponents.

The Plan includes initiative and project recommendations that specifically focus on enhancements and advancements that address specific security needs and establish a long-term (three-to-five year) strategic direction for the Information Assurance (IA) and Cyber Security (CS) Program.

As noted earlier, the strategy outlined in this Plan is a companion document meant to complement the Office of Information Management and Technology's (OIMT's) IT/IRM Transformation Architecture. The IA and CS Strategic, Program Management, Continuity of Operations and Disaster Recovery, Privacy, and Governance plans identify much of the foundational structure. The management roles, responsibilities, and oversight functions; risk-management processes; compliance, security, and efficiency goals; and foundational program and project management processes necessary to support the strategic direction and tactical efforts are identified in this Plan.

In preparing the Plan, the authors evaluated the current state of IA and CS within the State at the department, division, and branch levels. Using legislated requirements, educational studies, industry and government best practices and planning documents, department and organizational commitments and lines of business (LOBs), and the experience and knowledge of the team members to build a list of prioritized initiatives, a strategy was developed that will help to focus State's technology efforts.

By adopting any of the initiative recommendations identified, a significant improvement the State's security posture will be achieved.

All of the recommended initiatives represent significant investments of both capital and human resources; however, the benefits derived in implementing these initiatives greatly outweigh the potential risks associated with damage to State's reputation, mission activities, and public trust.

2 INTRODUCTION

2 INTRODUCTION

This Plan defines and prioritizes a number of IA and CS initiatives that the State must undertake to enhance the protection of information. While referred to as a strategy, the Plan is more properly a list of strategic investments. In preparing the Plan, the authors have made a strong effort to consolidate previously identified projects (where practical), provide scope and definition to each of the identified efforts, identify the general risks addressed by the initiative, and provide a foundation that can later be refined by formal project teams. In addition, to support a higher-level evaluation of which initiatives can be undertaken and when, the Plan attempts to identify any significant dependencies associated with the initiatives.

2.1 BACKGROUND

The State's various mission objectives, geographically diverse organizational structures, and many partnerships present unique technical challenges. The effectiveness of the techniques currently employed within the departments to address risks to information is inconsistent, and the use of the technologies has not been used to maximum capabilities. Former IA and CS programs and related management plans, strategies, processes, and initiatives established a succession of progressively elaborative IA and CS improvement tactics that built a sound foundation and established direction for the State's IA and CS program.

The approach in this Plan combines, defines, and prioritizes a list of multiple investments intended to consolidate all State departmental IT security initiatives into a shorter, more concise list of key investment efforts. Although it is still not a short list, the remaining initiatives can be evaluated with other IT/IRM program projects and available resources to decide which can be realistically accomplished. The risk assessments outlined in this Plan can provide key IT, mission, and stakeholder communities with an important decision-making tool when evaluating and documenting the risks associated with IA and CS projects that cannot or will not be completed.

This Plan builds heavily upon the development and deployment of a multi-layered defense strategy: the Acceptable Risk Management (ARM) and the IT Certification and Security Experts ISC2® Certified Information System Security Professional (CISSP) 10 Domains of Information Assurance.[1]

2.2 CURRENT AND EMERGING CYBER SECURITY THREATS

Cyber threats pose a critical national and economic security concern due to the continued advances in—and growing dependency on—the IT that underpins nearly all aspects of modern society. Data collection, processing, storage, and transmission capabilities are increasing exponentially; meanwhile, mobile, wireless, and cloud computing bring the full power of the globally connected internet to a myriad of personal devices and critical infrastructure. Because of market incentives, innovation in functionality is outpacing innovation in security, and neither the public nor private sector has been successful at fully implementing existing best practices.

The impact of this evolution is seen not only in the scope and nature of cyber security incidents, but also in the range of actors and targets. In the last year, we observed increased breadth and sophistication of computer network operations (CNOs) by both state and non-state actors. Our technical advancements in detection and attribution shed light on malicious activity, but cyber intruders continue to explore new means to circumvent defensive measures.

Among state actors, China and Russia are of particular concern. As indicated in the October 2011 biennial economic espionage report from the National Counterintelligence Executive, entities within these countries are responsible for extensive illicit intrusions into U.S. computer networks and theft of U.S. intellectual property.

Non-state actors are also playing an increasing role in international and domestic politics using social media technologies. We face a cyber-environment where emerging technologies are developed and implemented faster than governments can keep pace, as illustrated by the failed efforts at censoring social media during the 2011 Arab Spring revolutions in Tunisia, Egypt, and Libya. Hacker groups, such as Anonymous and Lulz Security (LulzSec), have conducted distributed denial of service (DDoS) attacks and website defacements against the government and corporate interests they oppose. The well-publicized intrusions into NASDAQ and International Monetary Fund (IMF) networks underscore the vulnerability of key sectors of the U.S. and global economy.

Hackers are also circumventing network security by targeting companies that produce security technologies, highlighting the challenges to securing online data in the face of adaptable intruders. The compromise of U.S. and Dutch digital certificate issuers in 2011 represents a threat to one of the most fundamental technologies used to secure online communications and sensitive transactions, such as online banking. Hackers also accessed the corporate network of the computer security firm RSA in March 2011 and exfiltrated data on the algorithms used in its authentication system. Subsequently, a U.S. defense contractor revealed that hackers used the information obtained from RSA to access its network.

[1] *International Information Systems Security Certification Consortium, "CISSP Domains, 2012." https://www.isc2.org/cissp-domains/default.aspx [1 May 2012]*

2.2.1 OUTLOOK FOR 2013-2015

We assess that CNO is likely to increase in coming years. Two of the greatest strategic challenges regarding cyber threats are:

1. The difficulty of providing timely, actionable warning of cyber threats and incidents, such as identifying past or present security breaches, definitively attributing them, and accurately distinguishing between cyber espionage intrusions and potentially disruptive cyber-attacks.

2. The highly complex vulnerabilities associated with the IT supply chain for networks.

3. The increase of "Advanced Persistent Threats (APTs)" from outside entities constitute a major challenge for information assurance and cyber security professionals. APTs require a high degree of stealthiness over a prolonged duration of operation in order to be successful. The attack objectives therefore typically extend beyond immediate financial gain, and compromised systems continue to be of service even after key systems have been breached and initial goals reached. Implementation of proactive continuous monitoring of network perimeter, computer systems and infrastructure is therefore critical for the survivability of state services and citizen support.

2.2.2 COUNTERINTELLIGENCE

Foreign intelligence services (FIS) are constantly developing methods and technologies that challenge the ability of information assurance professionals to protect data, information systems, and infrastructure. The changing, persistent, multifaceted nature of these activities makes them particularly difficult to counter.

Given today's environment, the authors assess that the most menacing foreign intelligence threats in the next two to three years will involve:

- Cyber-enabled Espionage. FIS have launched numerous computer network operations targeting various government agencies, businesses, and universities. Many intrusions into U.S. networks are not being detected or are being detected after large amounts of sensitive data have already been extricated. Although most activity detected to date has been targeted against unclassified networks connected to the internet, foreign cyber actors have also begun targeting classified networks.

- Insider Threats. Insiders have caused significant damage to government interests from the theft and unauthorized disclosure of classified, economic, and proprietary information and other acts of espionage. Trusted insiders who use their access for malicious intent represent one of today's primary threats to networks.

- Espionage by FIS. The U.S. Government reports that many foreign countries are aggressive and successful purveyors of economic espionage against the U.S. Foreign Intelligence Operations, including cyber capabilities, have dramatically increased in depth and complexity in recent years. FIS will remain the top threat to the United States and state interests in the coming years.

- Hacktivism (Hacker Activism). This is defined as "The activity of using computers to try to achieve social or political change."[2] Hacktivist organizations accounted for 58 percent of all data stolen in 2011.[3]

- Cyber Cartels (aka Cyber Mafia). These large, dispersed organized cybercrime syndicates use sophisticated and persistent attempts to gain access to private computer networks and systems to steal information for personal gains (e.g., identity theft and blackmail).

Evolving business practices and IT will provide even more opportunities for trusted insiders, hackers, and others to collect sensitive data. Corporate supply chains and financial networks will increasingly rely on global links that can be exploited by foreign collectors, and the growing use of cloud data processing and storage may present new challenges to the security and integrity of sensitive information.

2.3 SCOPE

The Plan presented in this document establishes a prioritized list of statewide departmental IA and CS investments and identifies a number of supporting rationale, including the risk reduction benefits for each. Recommended initiatives are generic to program needs and made without regard to specific department needs or future technologies. Initiatives have been evaluated for their do-ability; initiatives with higher project risk were not as highly favored as those with more mature implementation technologies. Although this Plan prioritizes IA and CS initiatives, it recognizes that the recommendations may not be approved or assigned to project teams as prioritized. Therefore, the Plan assumes that initiatives are reviewed by the IA&P-AWG prior to approval by the CIOC, IPSC, ELC, and EA-AWG, investments will be assigned to project managers, and then detailed project and implementation plans will be developed.

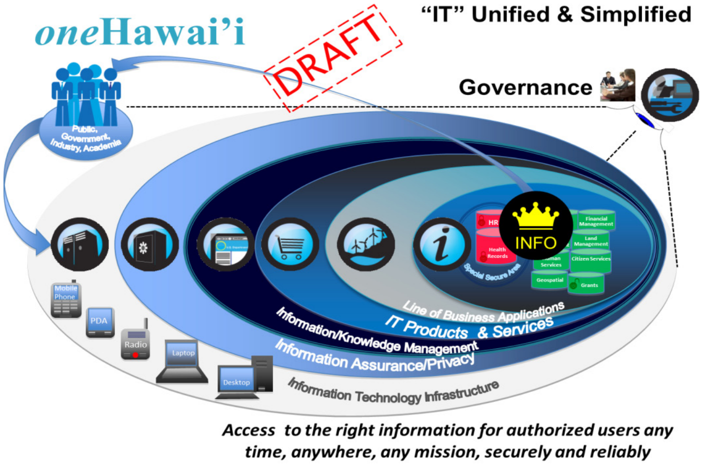
The Plan supports a multi-layered security model and identifies a number of technical and management-level recommendations that will improve the security posture of State. This document is not intended to be an implementation plan for the recommendations provided. The selection of any recommendation to be implemented, completion schedules, resource allocation, budgeting, and impact analysis is beyond the scope of this plan. As recommendations are reviewed by the IA&P-AWG and approved by the CIOC, each will be assigned to a project manager and implementation plans will be developed.

[2] Hacktivism, as defined in the Cambridge Business English Dictionary, 2011 Edition

[3] "2012 Data Breach Investigations Report." Verizon RISK Team, March 14, 2012. .http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf?CMP=DMC-SMB_Z_ZZ_ZZ_Z_TV_N_Z037 [1 Jun. 2012]

2.4 ALIGNMENTS

This document aligns with and complements the IA and CS Program Management Plan, materials presented to the CIOC during recent briefings, departmental priorities, the Governor's New Day Plan initiatives and priorities, and current legislation. Specifically, it is intended to align with the priorities outlined in the Governor's New Day Plan and the OIMT's IT/IRM Transformation Agenda pending legislative review and funding.



Access to the right information for authorized users any time, anywhere, any mission, securely and reliably

Figure 1 - CIO's IT/IRM Transformation Vision

2.5 IA AND CS PROGRAM MANAGEMENT PLAN

This Plan complements the new IA and CS Program Management Plan, which defines departmental IA and CS program roles, responsibilities, and processes with respect to establishing IA and CS policy, standards, and operational/oversight functions. It establishes a framework for a common State risk-based approach that places emphasis on the control of likely (vs. less likely) risks and threats. This framework will ensure the safeguarding of organizational information assets while not ignoring other key factors, such as cost, performance, mission requirements, and efficiency. The framework will also establish and document a risk acceptance management chain based on program-level responsibilities and risk impact awareness by bringing risk management and acceptance processes closer to the program level with assurance statements supporting senior management's overall responsibilities.

This Plan's purpose is consolidation and prioritization of the improvement initiatives for implementation and commitment. Using the Risk Management Framework in the IA and CS Program Management Plan and associated governance, the processes will need to identify and accept residual risks as needed where remaining gaps exist. The IT/IRM governance processes will establish a set of those improvement initiatives that State believes are within our resources to implement and measure performance/success based on these. This Plan will identify opportunities for increased efficiencies, including specifying IA and CS services that are candidates for enterprise solutions. This Plan will also attempt to identify gaps in existing compliance functions, evaluate their related risks, and incorporate prioritized improvement strategies and risk reassessments into the Plan for continuous re-evaluation of the strategy.

2.6 PURPOSE AND BENEFITS

This document is intended to:

- Consolidate and replace previous departmental lists of priorities relating to IA & CS program functions and recommendations included in various departmental plans into a single coherent set of recommended initiatives. The proper prioritization[4] of the resulting consolidated list of recommended initiatives should be based on initiatives that:

  - First, contribute to both systemically improving security controls over information and information systems (as informed by both departmental and OIMT evaluations and assessments) and that relate to improving those aspects that adversely impact the ability to provide information in a reliable and secure way to support any mission.

  - Second, only contribute to systemically improving security controls over information and information systems (as informed by both departmental and OIMT evaluations and assessments).

  - Third, provide security operations to monitor continuously the status of security infrastructure in a proactive nature.

  - Fourth, provide information assurance guidance and align to future-state technology deployments in an Agile framework.

[4] Prioritization also attempts to take into account the appropriate sequencing of activities necessary to ensure that foundational capabilities exist to enable the success of dependent activities.

[5] This effort is a change in management approach aimed at efficiency improvements and cost avoidance. The goal of the change is to better select and manage IA resources and projects. An effective IA program will likely result in decreased costs through reduced risk of potential litigation or penalty associated with significant data breaches.

  - Fifth, contribute to security as an enabler to state business processes.
  - Lastly, contribute to improving security controls over information and information systems within individual department/branch IT security programs and specific information systems (as informed by both departmental and OIMT evaluations and assessments).
- Serve as the basis upon which comprehensive individual IA and CS initiative[5] project plans can be developed that will improve security and privacy controls:
  - Enhance compliance with State and Federal laws.
  - Reduce potential State/department liabilities.
  - Assist in the support of Federal and private grant proposals.
- Serve as a decision document in IT program-level planning and as a mechanism to improve resource planning, efficiency, and economies of scale by clarifying priorities and supporting integrated projects and enterprise solutions, including:
  - Provide a mechanism for the departments to collaborate on, implement, and establish priorities in a concerted and coordinated manner.

3
FUNDAMENTALS OF INFORMATION ASSURANCE RISK MANAGEMENT

3
FUNDAMENTALS OF INFORMATION ASSURANCE RISK MANAGEMENT

The management, assessment, and mitigation of risks to IT systems are a fundamental component of every organization's information assurance and cyber security program. An effective risk management process enables an organization to protect its information assets and supports its ability to carry out its mission successfully.

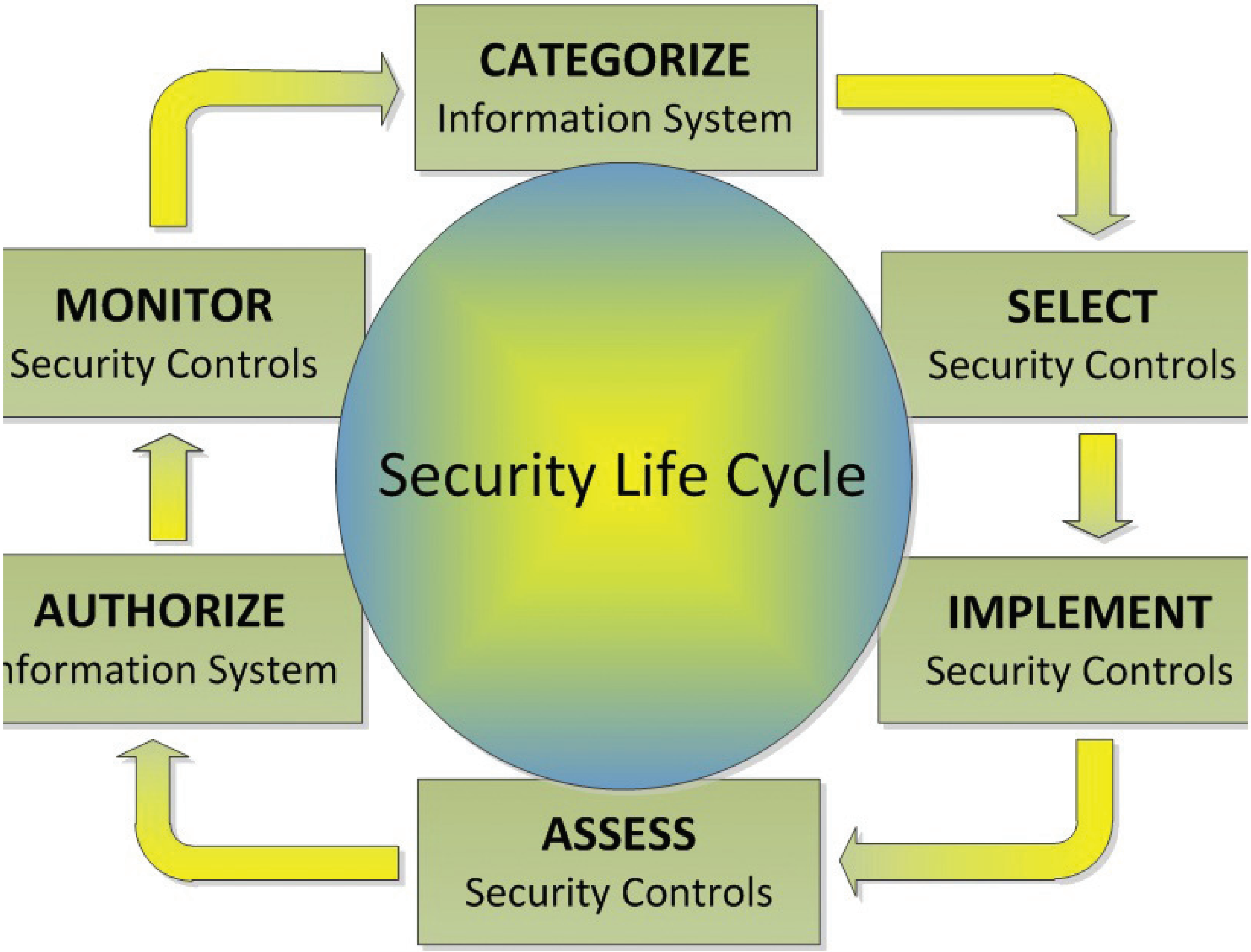


Figure 2 - Security Life Cycle

The following activities compose the Risk Management Framework. These activities are fundamental to the management of organizational risk and can be applied to both new and legacy information systems within the context of the System Development Life Cycle (SDLC) and the State of Hawai`i's Enterprise Architecture (EA).

Categorize the information system and the information processed; stored, and transmitted by the system, based on the potential impact to the organization should events occur to put the system and its information at risk. The organization assigns a security impact value (low, moderate, high) for the security objectives of confidentiality, integrity, or availability for the information and information systems that are needed by the organization to accomplish its mission, protect its assets and individuals, fulfill its legal responsibilities, and maintain its day-to-day functions.

Security categorization standards for information and information systems provide a common framework and understanding for documenting the potential impact to organizations or individuals should there be a breach of security (e.g., a loss of confidentiality, integrity, possession, utility authenticity or availability) to information or the information system. Federal Information Processing Standard (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems, can assist departments to determine the security category of data and information systems. The categorization process also promotes effective management of information systems and consistent reporting.

Select an appropriate set of security controls for the information system after determining the security categorizations. FIPS documents specify minimum-security requirements for information and information systems for seventeen security-related areas that represent a broad-based, balanced information security program. The 17 security-related areas encompass the management, operational, and technical aspects of protecting federal information and information systems. Furthermore, organizations must meet the minimum-security requirements by selecting an appropriately tailored set of baseline security controls based on an assessment of risk and local conditions including the organization's specific security requirements, threat information, cost-benefit analyses, or special circumstances.

To address minimum security requirements, the State will make use of security controls from "NIST SP 800-53, Recommended Security Controls for Federal Information Systems," summarized[6] below. This publication provides a catalog of controls that departments may select to protect their information systems in accordance with their missions and business requirements. An initial baseline set of security controls is determined based on the impact analysis conducted under the provisions of FIPS standards. Departments can tailor and supplement the selection of baseline security controls, based on their assessment of risks. Guidance on tailoring the baseline controls is provided by NIST.

Table 1 - Security Controls Classes, Families, and Identifiers

Identifier	Family	Class
AC	Access Control	Technical
AT	Awareness and Training	Operational
AU	Audit and Accountability	Technical
CA	Security Assessment and Authorization	Management
CM	Configuration Management	Operational
CP	Contingency Planning	Operational
IA	Identification and Authentication	Technical
IR	Incident Response	Operational
MA	Maintenance	Operational
MP	Media Protection	Operational
PE	Physical and Environmental Protection	Operational
PL	Planning	Management
PS	Personnel Security	Operational
RA	Risk Assessment	Management
SA	System and Services Acquisition	Management
SC	System and Communication Protection	Technical
SI	System and Information Integrity	Operational
PM	Program Management	Management

[6] *"NIST 800-53: Recommended Security Controls for Federal Information Systems." National Institute of Standards and Technology, 2011.*

Implement the security controls in the information system. Various Federal guides provide assistance in implementation of security controls; the State will use the NIST Special Publication Checklists for IT Products (http://checklists.nist.gov/) whenever available or vendor best practice standards. Checklists of security settings are useful tools that have been developed to guide IT administrators and security personnel in selecting effective security settings that will reduce the risks and protect systems from attacks. A checklist, sometimes called a security configuration guide, lockdown guide, hardening guide, security technical implementation guide, or benchmark, is a series of instructions for configuring an IT product to an operational environment. Checklists can be effective in reducing vulnerabilities to systems, especially for small organizations with limited resources. IT vendors often create checklists for their own products, but other organizations such as consortia, academic groups, and government agencies have also developed them.

Assess the security controls using appropriate methods and procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. The IA and CS Division will provide certification services to assist departments in meeting assessment requirements.

Authorize information system operation based on a determination of the risk to organizational operations, organizational assets, or to individuals resulting from the operation of the information system and the determination that this risk is acceptable. NIST SP 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems, discusses the steps leading to an official management decision by a senior agency official to authorize operation of an information system, accepting the risks to agency operations, agency assets, or individuals based on the implementation of an agreed-upon set of security controls. Certification and accreditation of information systems are required activities for federal agencies.

Monitor selected security controls in the information system on a continuous basis including documenting changes to the system, conducting security impact analyses of the changes, and reporting the security status of the system to appropriate organization officials on a regular basis.

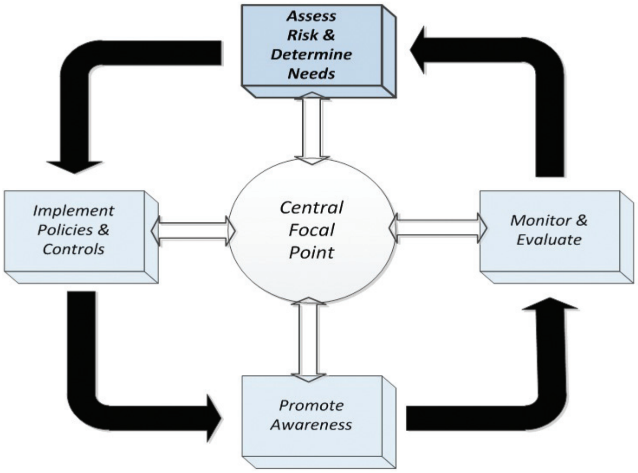


Figure 3 - Risk Management Cycle

Illustration from Information Security Risk Assessment - Practices of Leading Organizations

3.1 BASIC ELEMENTS OF THE RISK ASSESSMENT PROCESS

Whether they pertain to information security or other types of risk, risk assessments are a means of providing decision makers with information needed to understand factors that can negatively influence operations and outcomes and make informed judgments concerning the extent of actions needed to reduce risk. For example, bank officials have conducted risk assessments to manage the risk of default associated with their loan portfolios, and nuclear power plant engineers have conducted such assessments to manage risks to public health and safety. As reliance on computer systems and electronic data has grown, information security risk has joined the array of risks that governments and businesses must manage. Regardless of the types of risk being considered, all risk assessments generally include the following elements:

- Identifying threats that could harm and adversely affect critical operations and assets. Threats include such things as intruders, criminals, disgruntled employees, terrorists, and natural disasters.
- Estimating the likelihood that such threats will materialize based on historical information and judgment of knowledgeable individuals.
- Identifying and ranking the value, sensitivity, and criticality of the operations and assets that could be affected should a threat materialize in order to determine which operations and assets are the most important.

[7] *Information Security Risk Assessment - Practices of Leading Organizations. Supplemental Document. Washington D.C., U.S. General Accounting Office. 1999. page 6.*

- For the most critical and sensitive assets and operations, estimating the potential losses or damage that could occur if a threat materializes, including recovery costs.
- Identifying cost-effective actions to mitigate or reduce the risk. These actions can include implementing new organizational policies and procedures as well as technical or physical controls.
- Documenting the results and developing a plan of action and milestones for mitigating the any identified or residual risk.

There are various models and methods for assessing risk, and the extent of an analysis and the resources expended can vary depending on the scope of the assessment and the availability of reliable data on risk factors. In addition, the availability of data can affect the extent to which risk assessment results can be reliably quantified. A quantitative approach generally estimates the monetary cost of risk and risk reduction techniques based on 1) the likelihood that a damaging event will occur, 2) the costs of potential losses, and 3) the costs of mitigating actions that could be taken. When reliable data based on likelihood and costs are not available, a qualitative approach can be used by defining risk in more subjective and general terms such as high, medium, and low. This makes qualitative assessments depend more on the expertise, experience, and judgment of those conducting the assessment. It is also possible to use a combination of quantitative and qualitative methods.

3.2 ESTABLISH RELATIONSHIPS

The success of the Risk Management Framework is dependent upon the collaboration among the organization's many entities. Working together, senior leaders can make information risk decisions that ensure the organization's mission and business activities remain functional while also maintaining an acceptable security posture. The Information Security Program Office reaches out to the organization's information owners/information system owners to provide adequate guidance and direction on the categorization process. In addition, the Information Security Program Office develops and maintains relationships with the EA group, the Capital Planning personnel, and the technical operations personnel. 3.3 Develop Statewide Categorization Guidance

Information security programs should develop categorization guidance that supplements the existing guidance provided by Federal, State, and local compliance requirements and provides organization-specific procedures and documentation, approval, and reporting requirements. The specific guidance should address how information owners/information system owners:

- Integrate the categorization process into the system development life cycle.
- Handle new information types.
- Conduct the categorization process for their individual information systems.
- Document the categorization decision in the system security plan.
- Gain approval for the categorization decision.
- Report the categorization decision.
- Maintain the categorization decision by periodically validating that the categorization decision has not changed.

3.4 IDENTIFYING TYPES OF RISKS

Risks are very specific to the location, type of enterprise, and the size of the enterprise. A large multi-national enterprise will have very different risks than a smaller localized enterprise.

The first step in the risk assessment and analysis is to review the types of risks involved with a specific enterprise. There are four basic types of threat categories that can affect an enterprise: the insider, external, man-made, and natural disaster.

The insider threat is when the physical perimeter of the enterprise is compromised; this can be by an intruder, as when Ethan Hawk and company infiltrate the CIA offices in Mission Impossible. It is also when a current, trusted employee bypasses the in-place security protocols to gain access to information for which they do not have a need-to-know requirement.

External threats are less under control of the enterprise because they are instigated outside the network perimeter by individuals looking to do harm to the enterprise. Crackers/hackers are the typical category of external threats.

A sub-category of both internal and external threats is the man-made threat. The man-made threat can be categorized as a physical attack or accidents that affect the enterprise from performing business activities. Typical examples of man-made threats are the Transportation Security Authority (TSA) missing the shoe bomb scares in 2001 and 2009,[8] the accidental explosion of a power plant in Connecticut[9] during final stages of construction, and the explosion of the oil platform in the Gulf of Mexico.

Natural disaster threats are typically covered by the Business Continuity Process (BCP) or Disaster Recovery (DR) arenas of security, but are still just as relevant depending on the location(s) of the enterprise. For example, a New York office is more susceptible to a hurricane, but less likely to be disrupted by a tornado.

[8] *Richey, Warren, "Echoes of 2001 shoe bomber in Detroit attack – CSMonitor." December 28, 2009. The Christian Science Monitor. http://www.csmonitor.com/USA/Justice/2009/1228/Echoes-of-2001-shoe-bomber-in-Detroit-attack. [May 8, 2010].*

[9] *"Five dead in Middletown explosion, at least 12 injured, WTNH.com Connecticut." February 29, 2010. WTNH television. http://www.wtnh.com/dpp/news/middlesex_cty/middletown-power-plant-explosion. May 8, 2010.*

Table 2 - Identified Risks

Threat Type	Threat	Exploit/Vulnerability	Exposed Risk
Insider	Intruder	No security guard or controlled entrance	Theft
External	Hacker	Misconfiguration of firewall	Stolen credit card information
Internal	Current employee	Poor accountability; no audit policy; no security awareness program	Loss of integrity; altered data
Natural Disaster	Fire	Insufficient fire control	Damage or loss of life
External	Virus	Out-of-date antivirus software	Virus infection and loss of productivity
External	Spam overload e-mail system	No spam filtering	Loss of productivity
Internal	Hard drive failure	No data backup	Data loss and unrecoverable downtime
Man-made	Weapons of mass destruction; e.g., car bomb; package bomb; biological threat	No external facility monitoring; insufficient physical perimeter; no physical inspection of incoming packages	Data loss and unrecoverable downtime
Man-made	Accidental explosion	Non-compliance to OSHA requirements; bad construction practices	Loss of life; disruption of business; loss of reputation; environmental disaster

Once a list of risks to the enterprise is determined, the next step is to look at the methods and tools that can be used to determine what risks are the highest priority and/or will bring the greatest return on investment.

3.5 RISK CATEGORIES

This Plan discusses the prioritization of IA initiatives in terms of risks. The following generalized risk categories provide a basis for that discussion. A description has been provided in an attempt to clarify the types of risks included within each of the categories. The risks are not ordered by any weighting of importance nor are they equal in all applications.

1. Information Exposure/Loss: includes risks associated with the intentional or unintentional loss, theft, compromise, or disclosure of any type of sensitive department information or data, either in hard copy printed or soft copy electronic form that may be exploited by any unauthorized individual.

2. Unauthorized Use: includes risks associated with the intentional or unintentional use of any type of sensitive department information or data (in either hard copy printed or soft-copy electronic form), information system, or processes/procedures by an unauthorized individual.

3. Exposure to Contaminated Environments: includes risks associated with the intentional or unintentional exposure of any type of sensitive department cyber asset or information to potentially contaminated, untrusted, or insecure environments that may adversely affect the confidentiality, integrity, or availability of the exposed cyber asset or information. This can be done by the introduction of errors to information or data (in printed or electronic form); the introduction of malicious source code or software into an information system; or the introduction of unauthorized changes to automated processes/procedures.

4. Weak Processes: includes risks associated with the intentional or unintentional harm to any type of sensitive department information or data (either in hard copy printed or soft copy electronic form), information system, or processes/procedures resulting from inadequate controls either technical or manual (e.g., checks and balances, prone to human error and/or social engineering, etc.). These risks have the potential to affect the confidentiality, integrity, or availability of information or the information system adversely.

5. Unsecured Operating Environments: includes risks associated with the intentional or unintentional harm to any type of sensitive department information or data (either in hard copy printed or soft copy electronic form), information system, or processes/procedures resulting from inadequate controls either technical or manual (e.g., enabling the unauthorized modification of security controls within an information system increasing the systems vulnerability and susceptibility of information to compromise, enabling the unauthorized escalation of privileges to perform inappropriate functions on a system or to gain unauthorized access to information, etc.). These risks have the potential to impact the confidentiality, integrity, or availability of information or the information system adversely.

6. Loss of Public Confidence: includes risks associated with the intentional or unintentional harm to the reputation of the department and/or its leadership and the confidence of the public or senior government officials in the department's ability to conduct its mission effectively.

7. Exposure to Legal Action: includes risks associated with financial or non-financial legal actions taken against the department and/or its leadership. 3.6 Current Risk Assessment Methodologies

The two current base methodologies that are used by security professionals are the qualitative and quantitative methods. Each method is effective, but completely different in its approach to determining the level of risk. The issue is that each method could result in different outcomes.

Table 3 - Differences in Methodologies

Qualitative	Qualitative Quantitative
• Deals with descriptions	• Deals with numbers
• Designed to be a complete, detailed description	• Data is measureable
• Data is observed but cannot be measured	• Process uses mathematical tools
• Results are subjective	• Results are objective and testable
• Process is quicker	• More rigorous
• Less rigorous	

3.6.1 QUALITATIVE METHOD

The qualitative risk analysis is a process of assessing of the impact of the identified risks within an enterprise. By using this process, the priorities of vulnerabilities are determined to solve the risks based on the impact they could have on the enterprise. The definite characteristic of the qualitative method is the use, by the research team, of various subjective indexes such as ordinal hierarchy values: low-medium-high, vital-critical-important, benchmark, etc.

As described by Robert Jacobson in his analysis of Risk Assessment and Risk Management, once each risk is ranked, a risk matrix (shown in Table 4) can be developed.10

Table 4- Impact/Likelihood of Impact to the Enterprise Matrix

		Impact				
		Insignificant	Minor	Moderate	Major	Catastrophic
Likelihood	Almost Certain	🟧	🟧	🟧	🟥	🟥
	Likely	🟧	🟧	🟧	🟥	🟥
	Possible	🟧	🟧	🟧	🟧	🟧
	Unlikely	🟨	🟨	🟧	🟧	🟧
	Rare	🟨	🟨	🟧	🟧	🟧

[10] *Jacobson, Robert V., Computer Security Handbook, Volume 2, Risk Assessment and Risk Management. New York, NY: John Wiley and Sons, Inc., 2009. Chapter 62.*

In the example diagram in Figure 4, the point on the upper right is the risk that should be addressed immediately, while the lower left can be a risk that is accepted by management.

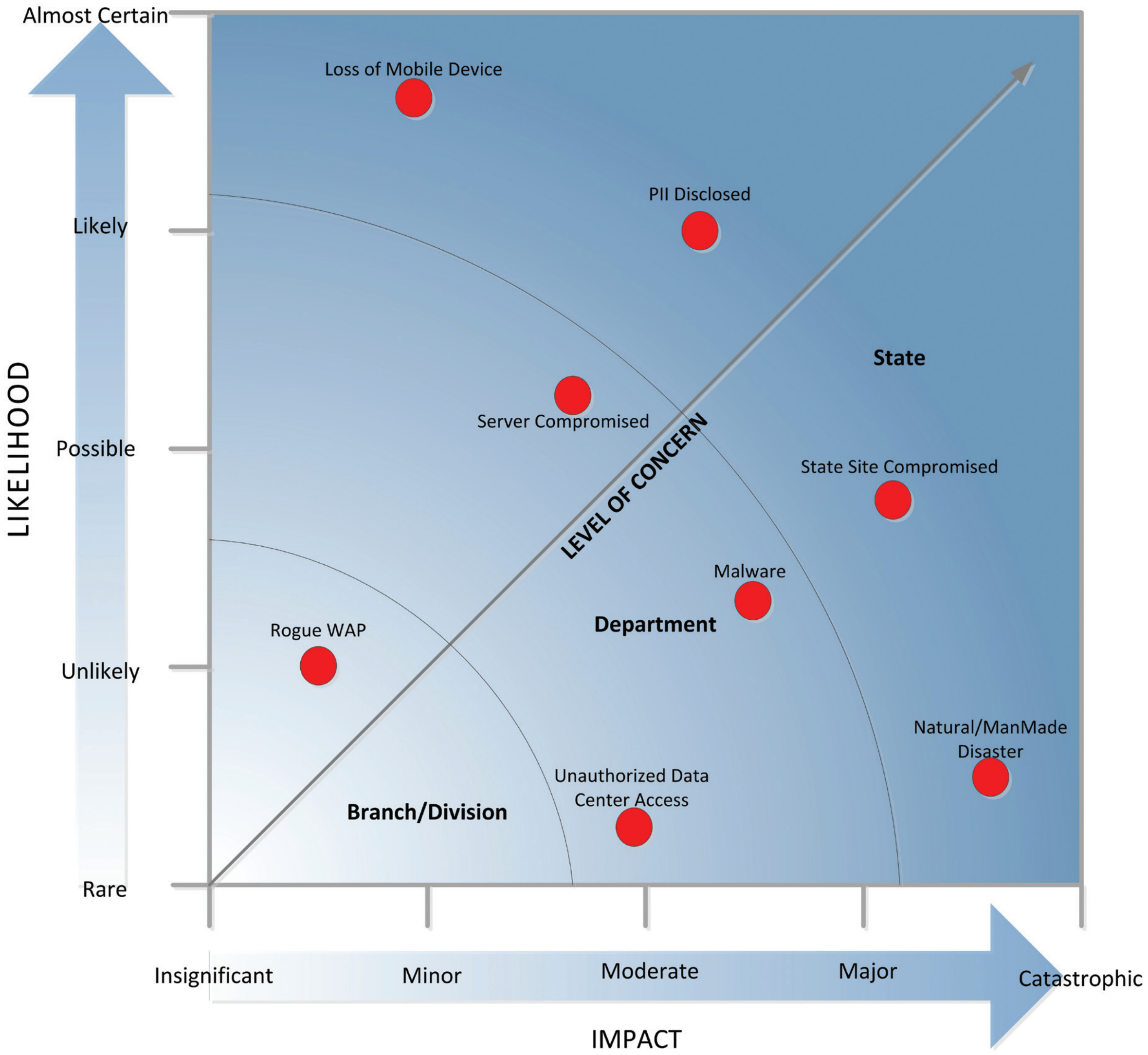


Figure 4 - Impact Assessment of Various Incidents to Enterprise

> "Estimating the likelihood of threat quantifiable as financial loss is difficult because it is based first of all on judgment and professional standing of the analyst."
>
> *Adrian Bogdanel Munteanu*

The statement above[11] describes the vital issue with the qualitative method. Typically, once the list of risks has been determined, the research is conducted by surveys and questionnaires. Even with a large cross section of the enterprise involved with the evaluation, the tendency will be for each functional area of the enterprise to rate their own areas high and vital. Once the surveys and questionnaires are collected and compiled, there is a high probability that the data will not identify a single risk or risks that need to be addressed. All the risks will have shown a high-vital mitigation need.

3.6.2 QUANTITATIVE METHOD

Through the quantitative risk analysis method, the assessment team can obtain some numerical results that express an approximate probability of each risk factor and its consequences on the objectives of the enterprise, but also the risks at the individual vulnerability level. The process uses several different mathematical techniques to evaluate the risks and make the determination based on the monetary loss if the risk occurs within a specific period.

[11] *Munteanu, Adrian Bogdanel, "Information Security Risk Assessment: The Qualitative Versus Quantitative Dilemma. Managing Information in the Digital Economy: Issues & Solutions," Proceedings of the 6th International Business Information Management Association (IBIMA) Conference, pages 227-232. June 19-21, 2006. (http://ssrn.com/abstract=917767)*

The most widely used mathematical models used in qualitative risk:

SLE = AV * EF

ALE = SLE * ARO

Table 5 - Factors in Risk Analysis Equation

Equation Element	Definition
Exposure Factor (EF)	The proportion of an asset's value that is likely to be destroyed by a particular risk (0% ≤ EF ≤ 100%)
Single Loss Expectancy (SLE)	The expected monetary loss every time a risk is exploited
Average Rate of Occurrence (ARO)	The probability that an exploitation of a risk will occur within a year (0.0 ≤ ARO ≥ 1.0)
Annual Loss Expectancy (ALE)	The monetary loss that can be expected for an asset due to a risk over a one-year period
Asset Value (AV)	A monetary value assigned to an asset at risk. This may be based on its actual cost, and/or the cost of its replacement.

Table 6 - Example Risk Analysis Table

Asset	Risk	AV	EF	SLE	ARO	ALE
Citizen database	Hacked	$432,000	74%	$320,000	.25	$80,000
Data files	User HDD failure	$9,450	17%	$1,650	0.9	$1,485
Domain controller	System failure	$82,500	88%	$72,500	.25	$18,125
E-commerce website	DDoS	$250,000	44%	$110,000	.45	$49,500

The problem of using the ALE to make the determination of risk is that, when the ARO is only evaluated at one loss per year and a risk occurs either during that year or future years, there can be considerable variance in the actual loss.

For example, using the second example in the table above, management decides, based on the low ALE value of the risk, not to implement the risk mitigation solution recommended, a tape backup solution.

The ARO is high (0.9), meaning that the likelihood of occurrence is high. With such a high potential, the chance for multiple occurrences during a single year will increase the actual ALE higher than what the risk analysis determined. So if a single enterprise with 10,000 employees has approximately 100 hard drive failures in a single year, the actual loss is 100 * $1,485 = $148,500. If the tape backup solution were only a capital cost of $50,000, then the risk must be ranked just behind the customer database risk.

Therefore, it is important to make sure when using the quantitative method of risk analysis not to look at the risk as a single point in time, but as a value that changes with the passage of time.

3.7 ALTERNATIVE RISK ASSESSMENT METHODS

3.7.1 PROBABILISTIC RISK ASSESSMENT (PRA)

To perform risk analysis in mechanical systems, the engineering community primarily uses a quantitative method of risk assessment. It looks at the concepts of "What can go wrong?," "What is most likely to occur?," and "What will be the consequences?"

By determining what can go wrong, the PRA then uses event tree and fault tree analysis to determine what lead to the failure. PRA then uses this information to determine the consequences of the failure.

An example might be the failure of an automatic teller machine (ATM) to dispense cash. To determine the possible reasons for the ATM's failure, the event tree and fault tree would be used. The consequences would be dissatisfaction of customers and loss of business.

3.7.2 FORENSIC ANALYSIS OF RISKS IN ENTERPRISE SYSTEMS (FARES)

FARES is a new risk-centric approach to risk analysis. The methodology takes a step back from traditional risk analysis, which looks at individual vulnerabilities, and looks at a broader view.

This approach uses both qualitative and quantitative aspects of risk analysis in combination instead of one or the other method.

Peter Stephenson mathematically defines risks in an enterprise system[12] as the following:

$$\rho = \Pi(\tau * v \Rightarrow \mu)$$

Information Systems Risk (ρ) is the probability (Π) that a threat (τ) will successfully exploit a vulnerability (v) to create an impact (μ).

Using this base equation, the basic concept of FARES is that risks consist of many vulnerabilities and threats that can be exploited. Attempting to identify and mitigate the multitude of vulnerabilities and threats is almost impossible to identify and manage. Creating larger supersets of vulnerabilities and threats makes the risk analysis and assessment a more manageable effort.

Instead of trying to identify individual software vulnerabilities, FARES suggests creating a superset using common criterion called software vulnerabilities and working towards the credible threats can exploit them. Next, look at the impacts that would be caused by a successful exploitation of the threats, and then countermeasures can be put into place to lessen or completely remove the impact to the enterprise.[13]

3.8 CHALLENGES ASSESSING INFORMATION SECURITY RISKS

Reliably assessing information security risks can be more difficult than assessing other types of risks, because the data on the likelihood and costs associated with information security risk factors are often more limited and because risk factors are constantly changing. For example:

- Data are limited on risk factors, such as the likelihood of a sophisticated hacker attack and the costs of damage, loss, or disruption caused by events that exploit security weaknesses.

- Some costs, such as loss of customer confidence or disclosure of sensitive information, are inherently difficult to quantify.

- Although the cost of the hardware and software needed to strengthen controls may be known, it is often not possible to estimate precisely the related indirect costs, such as the possible loss of productivity that may result when new controls are implemented.

- Even if precise information were available, it would soon be out of date due to fast-paced changes in technology and factors such as improvements in tools available to would-be intruders.

This lack of reliable and current data often precludes precise determinations of which information security risks are the most significant and comparisons of which controls are the most cost effective. Because of these limitations, it is important that organizations identify and employ methods that efficiently achieve the benefits of risk assessment while avoiding costly attempts to develop seemingly precise results that are of questionable reliability.

[12] *Stephenson, Peter R., "Forensic Analysis of Risks in Enterprise Systems." The Center for Digital Forensics Studies, Ltd. 2010. http://www.google.com/search?hl=en&source=hp&q=Forensic+Analysis+of+Risks+in+Enterprise+Systems&btnG=Google+Search&aq=f&aqi=&aql=&oq=&gs_rfai= [May 8, 2010]*

[13] *Ibid, page 4.*

Table 7 - CISSP 10 Domains of Information Assurance

Access Controls	Business Continuity and Disaster Recovery
A set of mechanisms (e.g. two-factor authentication, Personal Identification Numbers [PINs], card readers, etc.) that work in concert to create security architecture protecting information system assets	Addresses the preservation of the State's IT/IRM infrastructure in the face of major disruptions, natural or man-made, to normal business operations and guarantee continuity of government
Cryptography	Secure Application Development
The principles, means, and methods of disguising (encrypt/decrypt) information during the storage, use, or transmission of information during its life cycle with the intent to make a foe take extraordinary measures to recover the data	Security controls implemented and tested during the SDLC.
Physical Security	Operations Security
Addresses the threats, vulnerabilities, and countermeasures that can be utilized to protect an enterprise's resources and sensitive information physically. Includes site/facility design considerations, perimeter security, fire and security control mechanisms, etc.	Used to identify the controls over hardware, media, and the operators with elevated access privileges to any of these resources
Security Architecture and Design	Telecommunications and Network Security
The concepts, principles, structures, and standards used to design, implement, monitor, and secure operating systems, equipment, networks, applications, and those controls used to enforce various levels of security	Network structures, transmission methods, transport formats, and security measures to provide a secure infrastructure
Legal, Regulations, Investigations, and Compliance	Information Security Governance and Risk Management
Addresses computer crime laws and regulations; the investigative measures and techniques that can be used to determine if a crime has been committed and methods to gather evidence	Identifies the State's information assets and the development, documentation, and implementation of policies, standards, procedures and guidelines

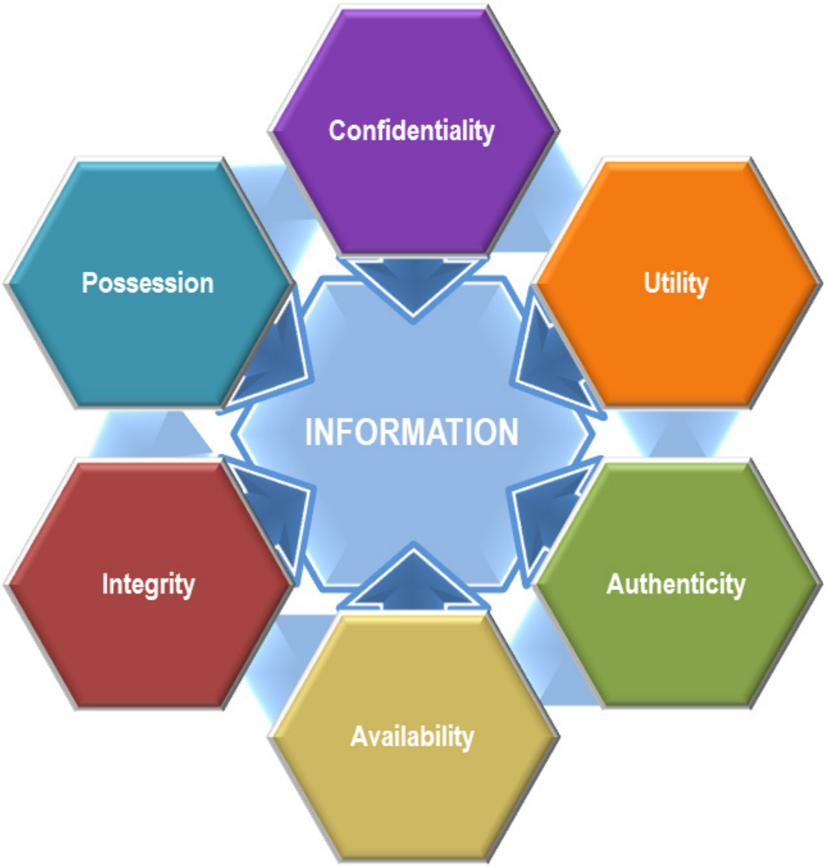


Figure 5 - Elements of Information Assurance and Cyber Security (Parkerian Hexad)

In 1998, Donn B. Parker expanded the original three fundamental elements of IA and CS into six elements of information security: Confidentiality, Possession (or Control), Integrity, Authenticity, Availability, and Utility.[14]

- Confidentiality – Limiting the access and disclosure to authorized users; at the same time, protecting information from unauthorized disclosure or not only the information but the existence of the information. An attacker cannot attack if the existence of the information is masked.
- Availability – Access to information is not restricted by time or circumstances; information anytime, for any mission, is the basic tenant of Business Continuity, Disaster Recovery, and Continuity of Government planning.
- Integrity – The trustworthiness or validity of the information being accessed or protecting it from modification by unauthorized users, corruption during transmission, or recovery of information from trusted sources.
- Possession – Also sometimes referred to as Control; maintaining control of the information. This includes physical controls and preventing copying or sending information to unauthorized users (e.g., using a single software license for an entire organization or software piracy).
- Authenticity – Misrepresenting information, repudiation, and misuse of information.
- Utility – Information maintains usefulness during its life cycle (e.g., an employee forgetting a decryption password or losing the master key to a data center).

This document also identifies multiple strategic investment recommendations, categorized in a multi-layer defensive solution framework and aimed at addressing inherent weaknesses in the State's internal and external security posture. While actions have been undertaken or are underway to address many of these earlier recommendations, some will be reiterated in this Plan where necessary to indicate the need for improved capabilities.

[14] *Parker, Donn B., Fighting computer crime: a new framework for protecting information. New York, NY USA: John Wiley & Sons. 1998.*

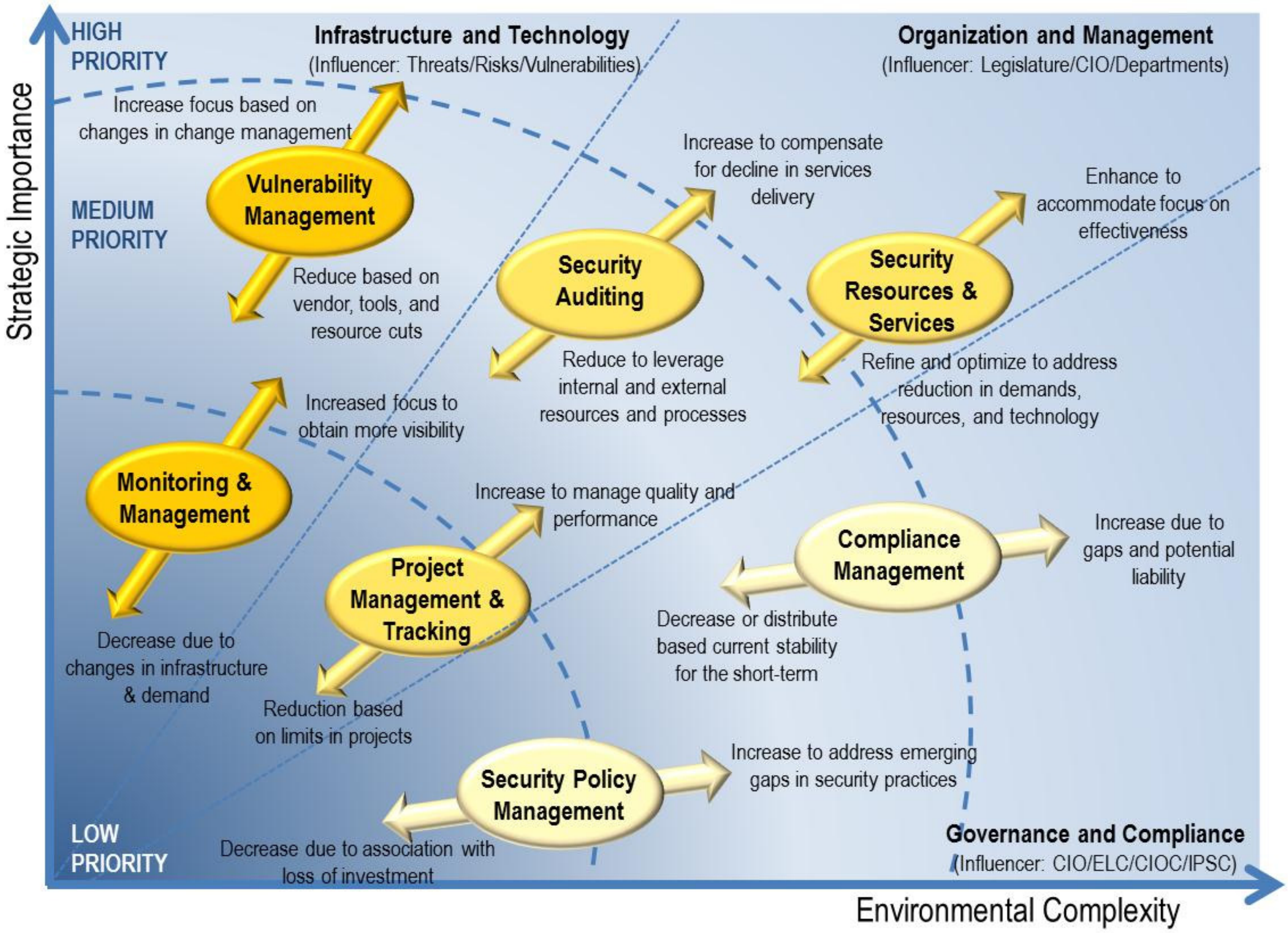

HIGH PRIORITY
Infrastructure and Technology
(Influencer: Threats/Risks/Vulnerabilities)
Organization and Management
(Influencer: Legislature/CIO/Departments)
Strategic Importance
Increase focus based on changes in change management
Vulnerability Management
Reduce based on vendor, tools, and resource cuts
MEDIUM PRIORITY
Increase to compensate for decline in services delivery
Security Auditing
Reduce to leverage internal and external resources and processes
Enhance to accommodate focus on effectiveness
Security Resources & Services
Refine and optimize to address reduction in demands, resources, and technology
Increased focus to obtain more visibility
Monitoring & Management
Decrease due to changes in infrastructure & demand
Increase to manage quality and performance
Project Management & Tracking
Reduction based on limits in projects
Compliance Management
Increase due to gaps and potential liability
Decrease or distribute based current stability for the short-term
Security Policy Management
Increase to address emerging gaps in security practices
Decrease due to association with loss of investment
LOW PRIORITY
Governance and Compliance
(Influencer: CIO/ELC/CIOC/IPSC)
Environmental Complexity

Figure 6 - Security Implementation Strategy Based on Importance vs. Complexity

Today's information systems[15] are complex assemblages of technology (e.g., hardware, software, and firmware), processes, and people working together to provide organizations with the capability to process, store, and transmit information in a timely manner to support various missions and business functions. The degree to which organizations have come to depend upon these information systems to conduct routine, important, and critical missions and business functions means that the protection of the underlying systems is paramount to the success of the organization. The selection of appropriate security controls for an information system is an important task that can have major implications on the operations and assets of an organization as well as the welfare of individuals. Security controls are the management, operational, and technical safeguards or countermeasures prescribed for an information system to protect the confidentiality, integrity (including non-repudiation and authenticity), and availability of the system and its information.

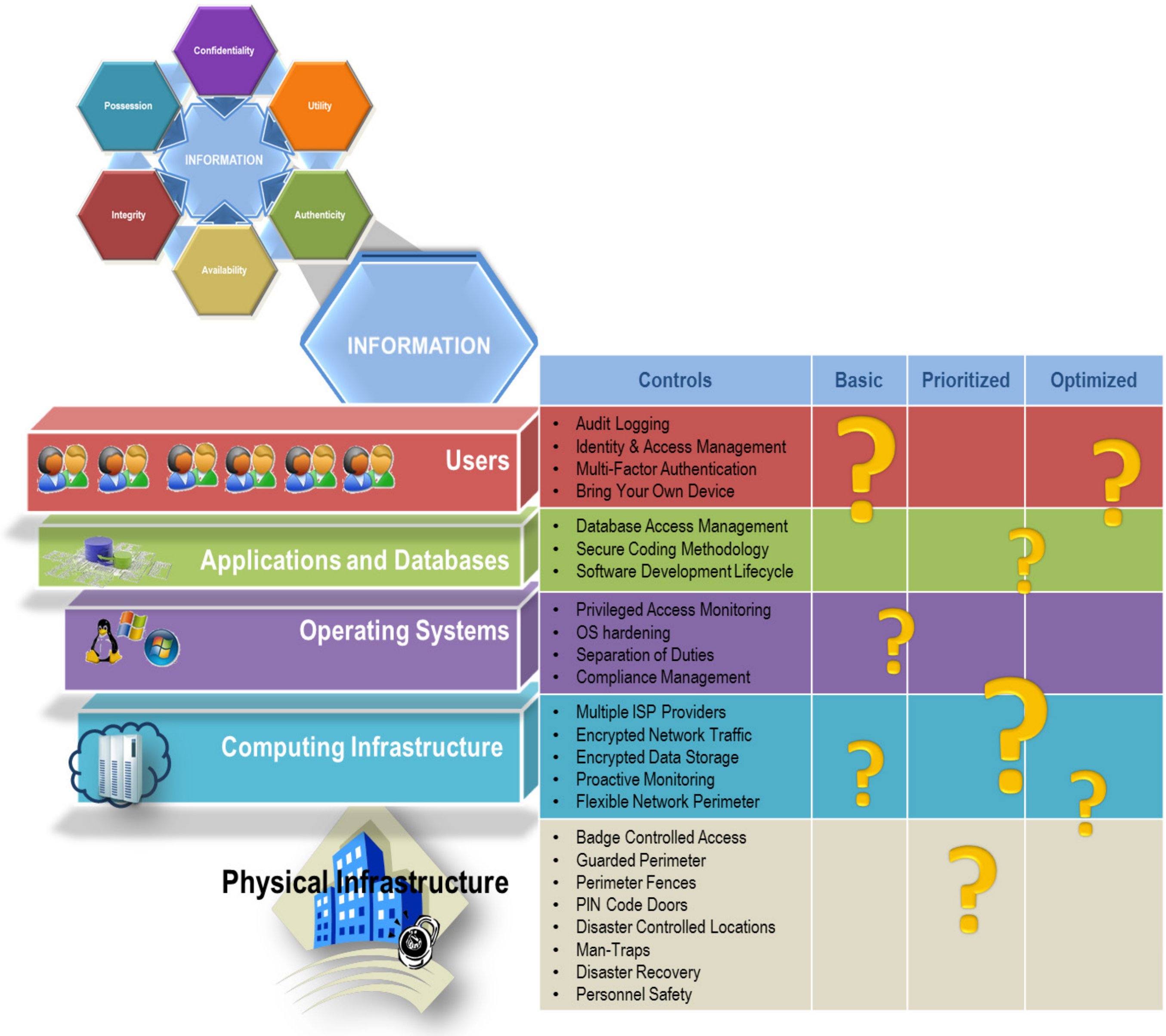
[15] An information system is a discrete set of information resources organized expressly for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Table 8 - Categories of Security Controls Related to Information Assurance

Control Types	Description
Physical Security	Preventive physical controls, traditionally "guards, guns and gates;" provide an environment to safely process information as well as barriers to unauthorized access to systems
Computing Infrastructure	Applies to all infrastructure components, networking, internet service providers (ISPs), servers, mobile devices, desktops, etc. sponsored by, developed for, or maintained or operated on behalf of the State, regardless of whether they are located at a State computing facility. The infrastructure also applies to pilot and proof-of-concept projects.
Operating Systems	An operating system (OS) is a set of software that manages computer hardware resources and provides common services for computer programs. The OS is a vital component of the system software in a computer system.
Applications and Databases	Security controls that cover software applications developed internally, by external acquisition, outsourcing/offshoring, or through hybrid approaches. These controls address all aspects of controls from determining information security requirements and protecting information accessed by an application or database to preventing unauthorized use and/or actions of an application.
Users	Ensure that unauthorized users do not get into the system and by encouraging (and sometimes forcing) authorized users to be security-conscious; for example, by changing their passwords on a regular basis. The system also protects password data and keeps track of who's doing what in the system, especially if what they are doing is security-related (e.g., logging in, trying to open a file, using special privileges).

Table 8 - Categories of Security Controls Related to Information Assurance

Level of Maturity	Description
Basic	At the basic level, processes are usually ad-hoc and chaotic. The organization usually does not provide a stable environment. Success in the organization depends on the competence and heroics of the people in the organization and not on the use of proven processes. Organizations often produce products and services that work; however, they frequently exceed the budget and schedule of their projects. Organizations are characterized by a tendency to over commit, abandon processes in the time of crisis and inability to repeat their past successes.
Prioritized	The organization has achieved all the specific and generic goals at the basic level. In other words, the projects of the organization have ensured that requirements are managed and that processes are planned, performed, measured, and controlled. The reflected discipline for the process helps to ensure that existing practices are retained during times of stress. When these practices are in place, projects are performed and managed according to their documented plans. Project requirements, processes, work products, and services are managed. The status of the work products and the delivery of services are visible to management at defined points. Commitments are established among relevant stakeholders and are revised as needed. Work products are reviewed with stakeholders and are controlled. The work products and services satisfy their specified requirements, standards, and objectives.
Optimized	The organization has achieved all the specific goals of the process areas assigned to maturity levels basic, managed and optimized, including the generic goals assigned to maturity levels basic and managed. Processes are continually improved based on a quantitative understanding of the common causes of variation inherent in processes. Optimization focuses on continually improving process performance through both incremental and innovative technological improvements. Quantitative process improvement objectives for the organization are established, continually revised to reflect changing business objectives, and used as criteria in managing process improvement. The effects of deployed process improvements are measured and evaluated against the quantitative process improvement objectives. Both the defined processes and the organization's set of standard processes are targets of measurable improvement activities. Optimizing processes that are agile and innovative depends on the participation of an empowered workforce aligned with the business values and objectives of the organization. The organization's ability to respond rapidly to changes and opportunities is enhanced by finding ways to accelerate and share learning. Improvement of the processes is inherently part of everybody's role and results in a cycle of continual improvement.



Controls	Basic	Prioritized	Optimized
• Audit Logging • Identity & Access Management • Multi-Factor Authentication • Bring Your Own Device	?		?
• Database Access Management • Secure Coding Methodology • Software Development Lifecycle		?	
• Privileged Access Monitoring • OS hardening • Separation of Duties • Compliance Management	?		
• Multiple ISP Providers • Encrypted Network Traffic • Encrypted Data Storage • Proactive Monitoring • Flexible Network Perimeter	?	?	?
• Badge Controlled Access • Guarded Perimeter • Perimeter Fences • PIN Code Doors • Disaster Controlled Locations • Man-Traps • Disaster Recovery • Personnel Safety		?	

Figure 7 - Information Assurance and Cyber Security Capability Maturity Model with Example Security Controls

Once employed within an information system, security controls are assessed to provide the information necessary to determine their overall effectiveness; that is, the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. Understanding the overall effectiveness of the security controls implemented in the information system and its environment of operation is essential in determining the risk to the organization's operations and assets, to individuals, to other organizations, and to the nation resulting from the use of the system.

Not all security controls listed in NIST 800-53 are applicable, as each IT/IRM environment is unique. To select individual security controls better, it is necessary to understand that there are specific categories of controls.

4
STRATEGIC INFORMATION ASSURANCE AND CYBER SECURITY GOALS AND OBJECTIVES

4

STRATEGIC INFORMATION ASSURANCE AND CYBER SECURITY GOALS AND OBJECTIVES

The IA initiatives identified in this Plan largely fall into one or more of six strategic goal areas:

- Protect Data – As demonstrated in a succession of well-publicized security events, the protection of privacy and other sensitive information is one of the most significant challenges faced in organizations today. This becomes even more challenging when addressed in the context of protecting access. Opening the information infrastructures to provide improved access to the right information for authorized users—anywhere, anytime, and any mission securely and reliably—is fundamental to State's ability to preserve and improve its mission capabilities. Meeting this objective; however, increases the complexities associated with protecting our sensitive information.

- Proactive Continuous Monitoring – The goal of continuous monitoring is to provide real-time awareness of a department's security posture, enabling departments to address threats and to remediate vulnerabilities proactively before they can be exploited.

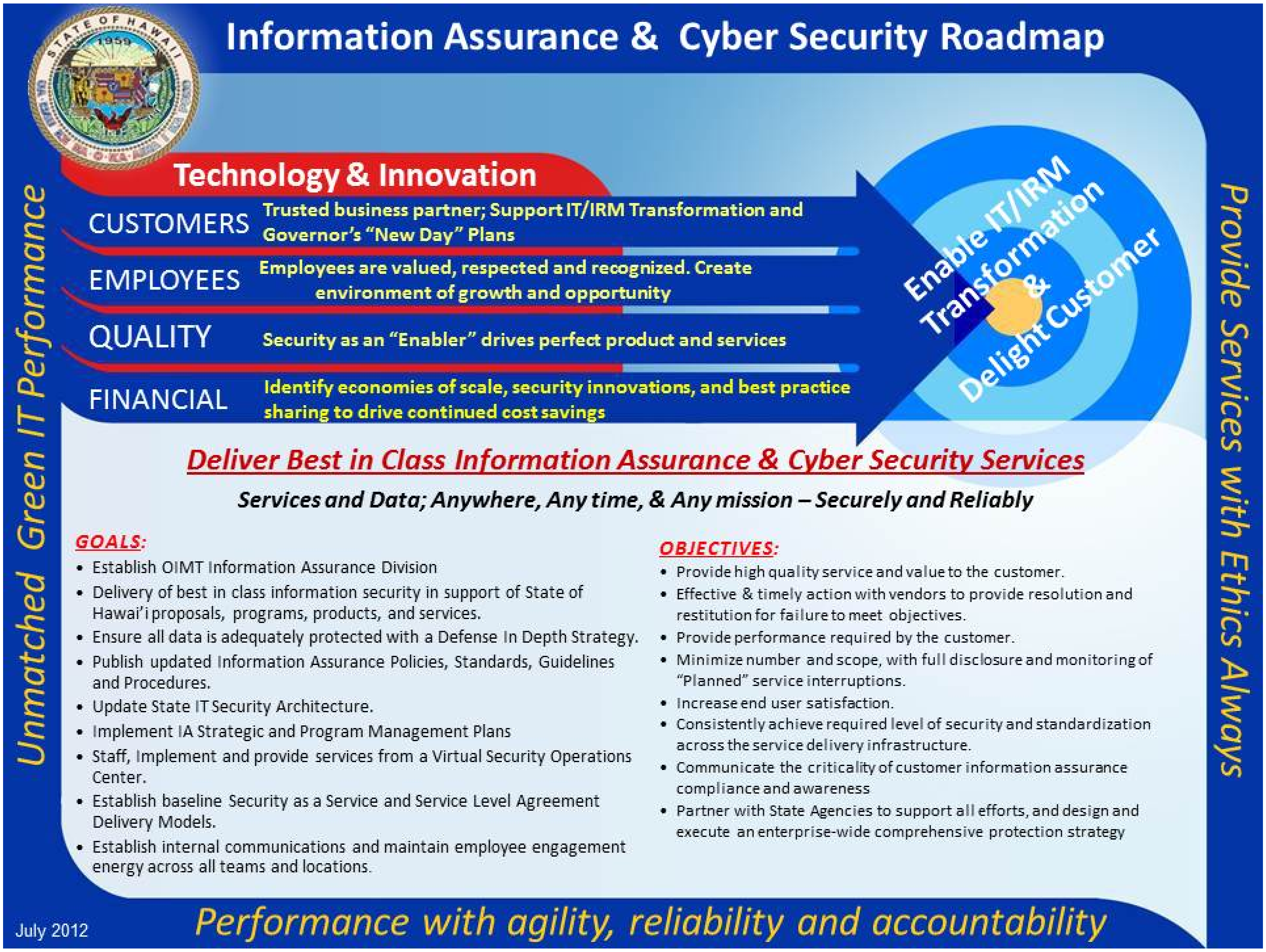
- Network Centric – The network-centric approach focuses on providing defense at the periphery. This is what many would consider the traditional approach to provide security to the enterprise. While this method of protection is still valid, a more radical approach to security must include the life cycle of data, from creation, how it is used when valid, its use during any archival or retention requirements, and through its proper method of destruction.

- Data Centric – The data-centric approach focuses on the data itself and where it lives: the database. Data-centric continuous monitoring protects the data by identifying and fixing database vulnerabilities before exploitation occurs.

- Protect Access – In meeting the two significant objectives of protecting authorized users' access to the right information, the State must first strengthen its ability to granularly establish and enforce access rules, and then tie these rules to its information assets so that only those individuals with rights to information have those rights. In addition, to address the access objective of reliability, the State must deploy secure, reliable, capacious, and diverse access solutions that allow users access to needed information—anywhere and at any time.

- Situational Awareness – To support an awareness of infrastructure or information risk related to configuration or patching weaknesses, exposure, attacks, and deliberate or accidental misuse, through implementation of security monitoring technologies and operational monitoring of these technologies.

The New Day Plan established a unity of purpose with One Team – One Mission – One Vision – One Set of Goals and Objectives. This Plan was one of the six focus areas identified as part of the proposed four phases to be completed over the next four years of the current administration.



Information Assurance & Cyber Security Roadmap

Technology & Innovation

CUSTOMERS	Trusted business partner; Support IT/IRM Transformation and Governor's "New Day" Plans
EMPLOYEES	Employees are valued, respected and recognized. Create environment of growth and opportunity
QUALITY	Security as an "Enabler" drives perfect product and services
FINANCIAL	Identify economies of scale, security innovations, and best practice sharing to drive continued cost savings

Enable IT/IRM Transformation & Delight Customer
Unmatched Green IT Performance
Provide Services with Ethics Always

Deliver Best in Class Information Assurance & Cyber Security Services

Services and Data; Anywhere, Any time, & Any mission – Securely and Reliably

GOALS:

- Establish OIMT Information Assurance Division
- Delivery of best in class information security in support of State of Hawai'i proposals, programs, products, and services.
- Ensure all data is adequately protected with a Defense In Depth Strategy.
- Publish updated Information Assurance Policies, Standards, Guidelines and Procedures.
- Update State IT Security Architecture.
- Implement IA Strategic and Program Management Plans
- Staff, Implement and provide services from a Virtual Security Operations Center.
- Establish baseline Security as a Service and Service Level Agreement Delivery Models.
- Establish internal communications and maintain employee engagement energy across all teams and locations.

OBJECTIVES:

- Provide high quality service and value to the customer.
- Effective & timely action with vendors to provide resolution and restitution for failure to meet objectives.
- Provide performance required by the customer.
- Minimize number and scope, with full disclosure and monitoring of "Planned" service interruptions.
- Increase end user satisfaction.
- Consistently achieve required level of security and standardization across the service delivery infrastructure.
- Communicate the criticality of customer information assurance compliance and awareness
- Partner with State Agencies to support all efforts, and design and execute an enterprise-wide comprehensive protection strategy

July 2012

Performance with agility, reliability and accountability

Figure 3 - Information Assurance and Cyber Security Roadmap

5 PERSPECTIVE ON INFORMATION ASSURANCE

5 PERSPECTIVE ON INFORMATION ASSURANCE

The most important aspect of effectively managing the risk to the organization's operations and assets associated with operating enterprise information systems is a fundamental commitment to information security on the part of the senior leadership of the organization. This commitment is the internalizing of information security, as an essential mission need. Fundamental commitment to information security translates into ensuring sufficient resources (both dollars and people) are available to provide an appropriate level of security for the organization's information systems. Information security must be a top priority within the enterprise and structurally embedded within the infrastructure of the organization. This implies that every new initiative within the enterprise from the development of corporate strategies and programs to the acquisition of goods and services incorporates information security considerations, preferably as early as possible in the system development life cycle process. Information security requirements must be considered at the same level of importance and criticality as the mainstream functional requirements established by the enterprise.[16]

In 2011, Gartner conducted a survey of CIOs in Federal, state, local, and private sector organizations to determine the current level of concerns about the security posture of organization's and where they saw the current threats in order to map these threats to available technology solutions.[17] The results are shown in Figure 9.

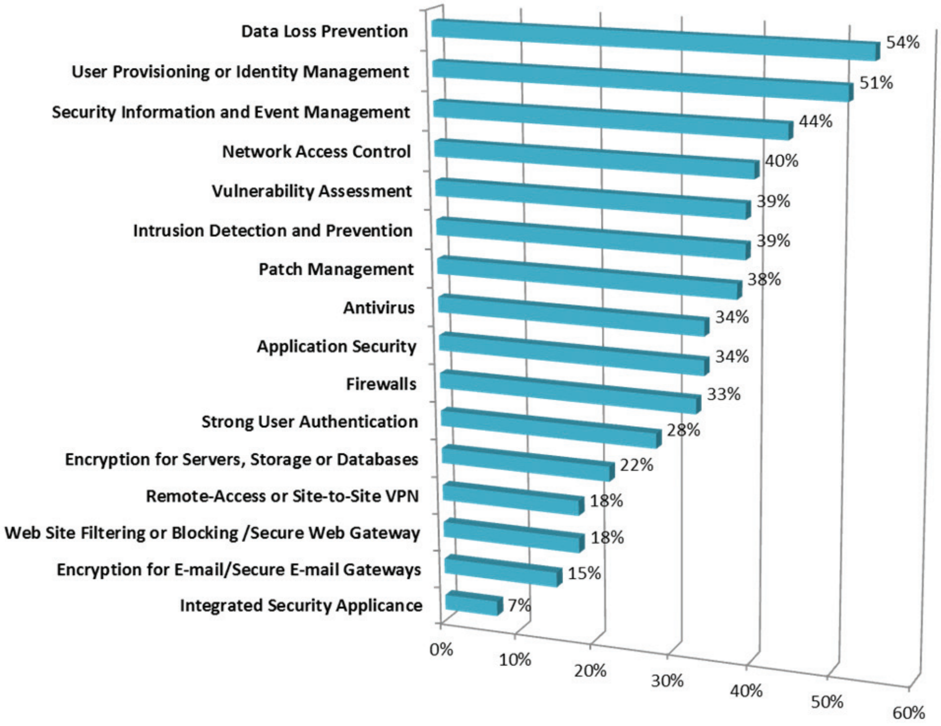


Figure 9 - CIO Top Information Assurance and Cyber Security Concerns (2011)

[16] *Ross, Dr. David, "Managing Enterprise Risk in Today's World of Sophisticated Threats." National Institute of Standards and Technology Washington: GPO. 2007.*

[17] *Gartner research at www.gartner.com*

5.1 COMMITMENT

To perform its mission effectively and efficiently, IT is an important component of each State organizational element's ability. Effective and efficient information security programs require clear direction and commitment from top management and administration. IA and CS are integrated functions that require effective organization and collaboration throughout the State. Protecting our electronic information and IT is the primary function of IT security. As an important mission enabler, IT security requires commitments on the part of both management and staff. These commitments will sometimes involve sacrifices. The loss of previously enjoyed computer use flexibilities that result in a gain in the overall level of protection against today's evolving IT threats can be the hardest hurdle for many organizations to make. Management's role is key to an organization's success in addressing the changes and impacts of any security improvement strategy.

As State employees, all of us have a shared responsibility to help maintain a strong security posture within our organizational environments. Nowhere is this more evident than with management. The security posture of State is only as strong as that of our weakest organizational component or user. This is evident in both outsider (external) and insider threat assessments conducted on the State's IT infrastructure. To be most effective, management must lead the way by demonstrating and emphasizing its commitment to improving the IT security of its organizations.

This Plan recommends departmental, division, branch, and office senior leadership re-emphasize that IT infrastructure contributes to our ability to accomplish our mission, and that every employee and contractor's actions are key to our overall success and contribute to the reliability and integrity of the infrastructure. IT security needs to be emphasized as an important means of protecting our IT infrastructure—one of the most important tools that we have today. To be most effective, IT security must be integrated into and considered in our everyday processes, planning, budgeting, and designs. IT security is not an IT responsibility, but every IT user's responsibility, from accountants, human resources specialists and scientists to budget analysts, planners, and engineers.

5.1.1 DEPARTMENT HEADS AND CIOS

Department Heads and CIOs are the offices of primary responsibility for information collected, maintained, and/or that has been identified as primarily utilized or owned by their respective departments. The CIOs may delegate operational management of these responsibilities by designation of a Department Information Security Officer (DISO) within their respective divisions. Vice Presidents may also designate other responsible parties to work with the DISO to assist in implementing this program. These designated individuals ensure information assets within their span of control have designated responsible parties (owners), that risk assessments are carried out for the departments, and that mitigation processes based upon those risks take place. The designated responsible party reports the status of the Information Security Program within the department as appropriate.

5.1.2 DIRECTORS, CHAIRS, MANAGERS, AND OTHER SUPERVISORS

Departments, divisions, branches, and attached agency directors, chairs, managers, and other supervisors responsible for managing employees with access to information and information systems are responsible for specifying, implementing, and enforcing the specific information security controls applicable to their respective areas. This includes ensuring all employees understand their individual responsibilities related to information security, and ensuring employees have the access required (and only the access required) to perform their jobs. Supervisors should periodically review all users' access levels to ensure they are still appropriate and take the appropriate action to correct discrepancies/deficiencies. Supervisors are required to notify Human Resources and the IT Help Desk proactively of any change in employment status that impact access requirements. Supervisors are also responsible for reporting suspected misuse or other information security incidents to the DISO, Chief Information Security Officer (CISO), and other appropriate parties.

5.1.3 CHIEF INFORMATION SECURITY OFFICER (CISO)

The State of Hawai`i CISO is designated as the Program Officer responsible for coordinating and overseeing the IA and CS Program. The CISO must work closely with the various departments throughout the State. The CISO may recommend that divisions/branches of specific departments delegate other representatives of the organization to oversee and coordinate particular elements of the Program.

The CISO also assists individuals who have the responsibility and authority for information (owners) with information security best practices relating to issues such as:

- Establishing and disseminating enforceable rules regarding access to and acceptable use of information resources
- Conducting/coordinating information security risk assessment and analysis; establishing reasonable security guidelines and measures to protect data and systems
- Assisting with monitoring and management of systems security vulnerabilities
- Conducting/coordinating information security audits
- Assisting with investigations/resolution of problems and/or alleged violations of state information security policies

Finally, the demonstration of commitment must be reflected in the allocation of resources, both human and capital, to the management and accomplishment of strategic security improvement goals. Without this important commitment, no significant progress can be made. 5.2 Communication Plan

Effective, efficient communication should involve a dialog. To ensure that communication lines remain open requires mutual respect for various disciplines and an equal voice in the process for all disciplines within the department, bureaus, and offices. Establishing that dialog means:

- Ensuring that all employees are engaged in the effort
- Ensuring opportunities for everyone to provide input to the process
- Recognizing that one solution may not work in every situation

When creating a new policy or recommendations and guidance, effective communication of these changes is often a last thought. Failure to implement new policy and directives throughout the state in a timely manner can often be attributed to the failure to raise awareness of the new guidance to the appropriate level in the IT workforce and user community. The lack of repetition and variety in the communication of policy perpetuates unawareness.

This Plan recommends the development of a comprehensive communication strategy to improve the dissemination and reception of IT security policies, procedures, standards, guidelines, directives and mandates. Specifically, the following areas of concern should be addressed in the communication strategy:

- Policy dissemination
- Management awareness
- Awareness training
- Consideration of the target audience
- Consideration of the culture of the various departments, divisions, branches, and offices within the State 5.3 Resource Management

To enable security programs at the department, division, branch, and office levels to succeed, this Plan recommends management establish realistic expectations and commit the appropriate resources. Those resources include adequate budget and staffing levels appropriate for the workload and the tools to assist in managing the security programs—asset/configuration management tools, automated certification and accreditation (C&A) tools, etc.

Separate recommendations with regard to resources are included elsewhere in the Plan. 5.4 Measuring Quality Effectiveness

The State of Hawai`i has instituted numerous improvement programs throughout the years. However, the sustainability and quality of the programs have, in many cases, deteriorated over time. Many programs provide quick-fix or check-the-box solutions and do not address the root causes. For any improvement or strategic plan to provide long-term value and not become shelfware, it must be continuously reviewed and re-evaluated for effectiveness.

It is recommended to review the Plan annually to ensure its relevance and effectiveness related to emerging technologies and threats.

6

INFORMATION ASSURANCE AND CYBER SECURITY DIVISION

6

INFORMATION ASSURANCE AND CYBER SECURITY DIVISION

There are key reasons the IA&CSP-AWG recommends establishing, defining, and documenting formal IA and CS roles and responsibilities. Even if roles have been defined, in this era of emphasis on security governance it is critical to document them as well. If information security roles are not clearly defined with the State and a roles and responsibilities clarification project is still missing in the overall IT/IRM governance structure, it is encouraged to use the following discussion to write a project justification memo to management.

Most departments have no dedicated security staff:

- There is simply not enough time to complete non-security tasks.
- Tasks are often put on hold as security functions are not seen as an immediate need.
- Time-sensitive tasks are completed as quickly as possible with no time for risk assessment, technology assessment, or training.

6.1 GARNER RESPECT AND RESOURCES

Documented role and responsibility statements are advisable for every department/division/branch and attached agencies, not just the IA and CS organization. Those organizational units with fully developed role and responsibility statements will enjoy greater respect and greater resources. Within many of the State's departments, information security is a new or still-undeveloped organizational function.

This means these same organizations are often missing documents that cover information security job descriptions, mission statements, and reporting relationships. When these roles and responsibilities are documented and approved, the information security function will be increasingly recognized as a legitimate and on-going organizational function, worthy of respect and its own share of organizational resources.

6.2 DEMONSTRATE TOP MANAGEMENT SUPPORT

One of the most important reasons to document role and responsibility assignments is to demonstrate top management support. Information security specialists often feel as though many people oppose what they are trying to do. Occasionally information security specialists must take an unpopular position, for example, postponing the cutover to a new software application until appropriate controls can be included. If the information security specialists are not going to be outvoted, outmaneuvered, and otherwise overruled, clearly documented top management support for the information security function must have been documented. With documented and approved roles and responsibilities, information security specialists can prevent or expediently resolve many arguments and get on with their work.

6.3 ESTABLISH FORMAL COMMUNICATION CHANNELS

At many organizations, the information security function has been repeatedly moved from department to department or distributed across many departments. Many of these departments may not have known what to do with the information security function. As a result, departmental management may not have seriously considered the recommendations offered by information security specialists. Consequently, management may have postponed or failed to fund a number of important information security projects. However, when roles and responsibilities for the information security function are specified and approved by top management, all this can quickly change. Then the information security function will have a real home; in other words, it will know where it fits into the organizational structure. In the course of defining a formalized and permanent home for the information security function, the ways that this function works with other internal groups will be defined. Then the information security function will have formal communication channels with top management that can be used to help get important projects underway.

6.4 FOSTER COORDINATED TEAM EFFORT TO SAFEGUARD INFORMATION

One additional important reason to document information security roles and responsibilities involves overcoming an erroneous viewpoint that information security is something that can be handled by specialists in the Information Security Department working alone. The job is way too big and way too important to be left to the Information Security Department. When roles and responsibilities are documented, specific people inside and outside the Information Security Department will be held accountable, and this in turn will cause them to become proactive. Without this accountability, in many cases they will wait until there is a problem, and then do their best to handle whatever has taken place. Today organizations can no longer approach information security with a fix-on-failure mentality. Research studies show that information security is ten times less expensive when it is built into application systems before they go into production instead of when it is added on after the systems have been placed in production. Stated a bit differently, when it comes to information security, proactive planning and management is considerably less expensive than reactive repair and correction efforts.

6.5 ENABLE BETTER ALLOCATION OF ORGANIZATIONAL RESOURCES

Many organizations are now turning to outsourcing firms to handle their information security needs. While some management responsibilities such as making final decisions about information security policies should ultimately rest on the shoulders of internal management, a considerable amount of the security work can be outsourced. If roles and responsibilities are not clearly established at the time that a contract is negotiated, the organization that contracted the outsourcing firm may find itself in a difficult spot. The outsourcing firm may claim that the requested service (such as forensic investigation of a system break-in) is not in the contract, and that the customer must pay an additional fee. All this of course assumes that the outsourcing firm has technically competent people available at the time they are needed.

Of course, other consulting firms can also be called in, but with any of these options, precious time will be wasted negotiating fees, defining the work to be done, etc. While all of these ad-hoc business arrangements are being made, a hacker could be on the loose inside an organization's internal network. To keep losses to a minimum, it is absolutely essential that roles and responsibilities for all important information security activities be defined in advance in outsourcing contracts.

On a related note, if management wishes to outsource some or all of the information security function or if management wishes to retain contractors, consultants, or temporaries to assist with information security, then roles and responsibilities must first be specified. Unless roles and responsibilities have been clearly defined, management will find it difficult or even impossible to draw up requests for proposals, legal contracts, outsourcing agreements, service level agreements (SLAs), and other documents adequately with these third parties. Thus, clear roles and responsibilities can be a significant enabler that allows management to better allocate organizational resources.

6.6 MINIMIZE ASSOCIATED COSTS FOR SECURITY AS A SERVICE (SECAAS)

A related business management reason to establish clear roles and responsibilities is that, in so doing, management will reduce costs to handle information security adequately. Through the specification of job descriptions, management can select and retain people who are adequately qualified, but not over-qualified. This will in turn help to keep salary costs down. Likewise, a number of organizations are increasingly taking the security tasks performed by Systems Administrators and assigning these tasks to new information-security-specific positions like Access Control System Administrator. Not only does this change provide better separation of duties, it also allows the organization to lower costs because the security-specific jobs often pay less than the Systems Administrator jobs. On a related note, when clear roles and responsibilities documentation exists, management will know exactly what types of training programs it should send internal staff to, and this will help avoid wasting resources on training that is not directly relevant to the jobs that the involved individuals perform.

6.7 REDUCE SINGLE POINT OF FAILURE

Rather than eliminating the need for human involvement, the new information systems that organizations are using today (such as ecommerce systems) are increasing the reliance on certain types of people with specialized skills. For example, if a critical technical person were to leave his or her employer abruptly, the organization might be hard pressed to continue certain technical computer operations without this person. This increased reliance on people with highly specialized skills and training can be reduced by backup personnel, cross training, sharing job responsibilities, documenting the work, and other tasks associated with the development of clear information security roles and responsibilities.

The IA field is still in its infancy when compared to the marketing, engineering, or accounting fields. While some interesting new technological solutions to information security problems are now on the market, in most organizations the achievement of effective information security critically depends on people. At this point in the evolution of the technology, many information security problems can only be handled by people. For example, there is no commercially available technological solution to protect against the social engineering (masquerading) threats that all organizations face. All too often, the people within an organization do not understand what management expects them to do, and this in turn will prevent the achievement of information security goals. When roles and responsibilities have been clarified and documented, and selected people are then appropriately trained, they can participate as essential members of the team that handles information security.

6.8 DEMONSTRATE COMPLIANCE

Another good reason to document roles and responsibilities is to demonstrate compliance with internal policies as well as external laws and regulations. Auditors and government examiners are impressed with documentation. It gives them the feeling that things are under control. A surprising number of modern laws include the requirement that information security roles and responsibilities must be specified. For example, in the United States, the Health Insurance Portability and Accountability Act (HIPAA) requires that organizations managing personal health information document information security related roles and responsibilities.

With clear documentation defining information security roles and responsibilities, an organization can show it is operating in a fashion that is consistent with the standard of due care. Being able to demonstrate this consistency may be very important in terms of reducing or eliminating management liability for losses and other problems. This documentation may help with a variety of liability concerns including computer professional malpractice and breach of management's fiduciary duty to protect information assets. One example of an authoritative statement of the standard of due care which includes the requirement to clearly specify information security roles and responsibilities is entitled Generally Accepted Information Security Principles (GASSP).[18]

Demonstrating compliance with the standard of due care can help shield the state from negligence and related liability claims.

6.9 INCREASE EFFICIENCY AND PRODUCTIVITY

Perhaps the most significant reason to establish and document clear roles and responsibilities involves increased productivity. Statistical studies of business economics indicate that about half of productivity growth over time comes from more efficient equipment, and about half comes from better trained, better educated, and better managed labor. Thus, the clarification and publication of information security roles and responsibilities can have a substantial positive impact on productivity, and thereby markedly improve cost savings. The information security field is a new area, and there is still great confusion about who should be doing what. For example, when a worker has his or her laptop computer stolen, to whom should the event be reported? Should a notice be sent to the Information Security Department, the Physical Security Department, or the Insurance Department? Maybe the notice should go only to the worker's manager? Without clear roles and responsibilities, users will unnecessarily spend time figuring out the answers to questions such as these. Likewise, if roles and responsibilities are clarified and documented, employees will not waste their time trying to figure out who to invite to certain meetings or who needs to sign-off on certain proposals.

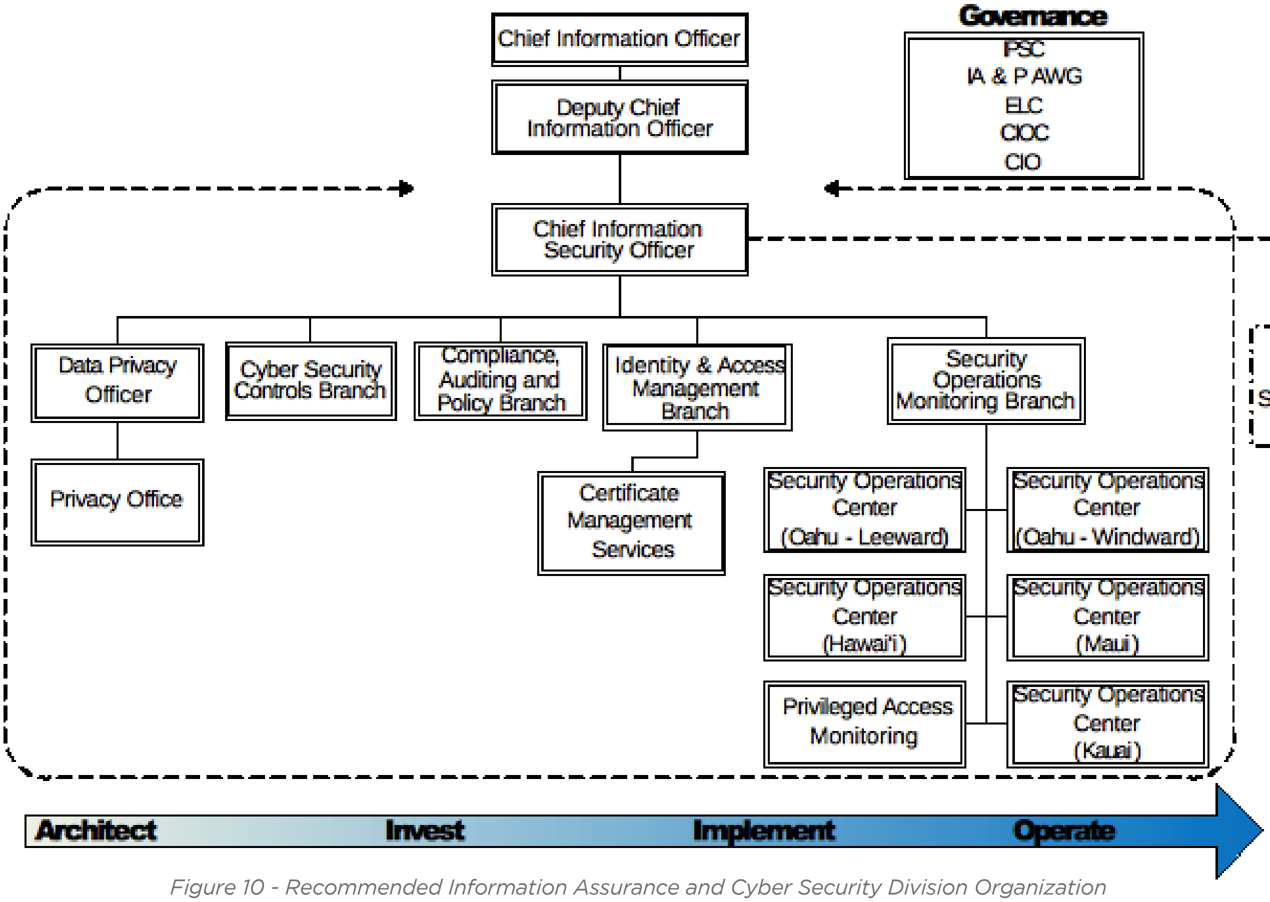

Chief Information Officer
Deputy Chief Information Officer
Governance
PSC
IA & P AWG
ELC
CIOC
CIO
Chief Information Security Officer
Data Privacy Officer
Privacy Office
Cyber Security Controls Branch
Compliance, Auditing and Policy Branch
Identity & Access Management Branch
Certificate Management Services
Security Operations Monitoring Branch
Security Operations Center (Oahu - Leeward)
Security Operations Center (Oahu - Windward)
Security Operations Center (Hawai'i)
Security Operations Center (Maui)
Privileged Access Monitoring
Security Operations Center (Kauai)
Department Information Security Officers (DISOs)
Architect
Invest
Implement
Operate

Figure 10 - Recommended Information Assurance and Cyber Security Division Organization

[18] *National Institute of Standards and Technology, Generally Accepted Information Security Principles for Securing Information Technology Systems. 1996, page 5.*

6.10 CYBER SECURITY CONTROLS BRANCH (CSCB)

Branch Services. Firewall (perimeter and server tier), web application firewall, DDoS protection/mitigation, DLP, IR management, and IDS/IPS

CSCB core functions:

- Data threats
- Access control threats
- Access and authentication controls
- Security gateways (firewalls, WAF, SOA/API, VPN)
- Security products (IDS/IPS, server tier firewall, file integrity monitoring, DLP, antivirus, anti-spam
- New security technology review and recommendations
- Denial of service attacks protection/mitigation
- Secure base services such as DNS and/or DNSSEC, DHCP, NTP, RAS, VPN, SNMP; management network segmentation and security
- Traffic/netflow analysis
- Integration with virtual technology layer

Challenges:

- Fluid network borders/perimeter (Instead of traditional clearly defined network boundaries, the borders between tenant and external networks can be dynamic and potentially blurred in a large-scale virtual/cloud environment.)
- Virtual segmentation of physical servers
- limited visibility of inter-virtual machine traffic
- Non-standard APIs
- Management of many virtual networks (VLAN in a complex environment; reliant on providers' policies and procedures)
- Separation of production and non-production environments
- Logical and virtual segregation of departmental networks/ systems/data

6.11 COMPLIANCE, AUDITING, AND POLICY BRANCH (CAPB)

Branch Services. Internal and/or external penetration test, application penetration test, host and guest assessments, firewall/IPS (security components of the infrastructure) assessments, and virtual infrastructure assessment

CAPB core functions:

- Governance — process by which policies are set and decision making is executed
- Risk management — process for ensuring that important business processes and behaviors remain within the tolerances associated with those policies and decisions
- Compliance — process of adherence to policies and decisions
- Policies can be derived from internal directives, procedures and requirements, or external laws, regulations, standards and agreements.
- Technical compliance audits — automated auditing of configuration settings in devices, operating systems, databases, and applications.
- Application Security Assessments — automated auditing of custom applications
- Vulnerability Assessments — automated probing of network devices, computers and applications for known vulnerabilities and configuration issues
- Penetration Testing — exploitation of vulnerabilities and configuration issues to gain access to a an environment, network or computer, typically requiring manual assistance
- Security/risk rating — assessment of the overall security/ vulnerability of the systems being tested, e.g., based on the OWASP Risk Rating Methodology

Challenges:

- Standards are on different maturity levels in the various sections
- Certification and Accreditation (C&A)
- Boundary definition for any assessments
- Skills of testers/assessors
- Accuracy
- Inconsistent ratings from different individuals/vendors
- Typically limited to known vulnerabilities

6.12 IDENTITY AND ACCESS MANAGEMENT BRANCH (IAMB)

The Identity and Access Management Branch (IAMB) should provide controls for assured identities and access management. IAMB includes people, processes, and systems that are used to manage access to enterprise resources (systems and data) by assuring the identity of an entity is verified and is granted the correct level of access based on this assured identity. Audit logs of activity such as successful and failed authentication and access attempts should be kept by the application/solution.

Branch Services. User-centric ID provider, federated IDs, web single sign-on (SSO), identity provider, authorization management policy provider, electronic signature, device signature, and user-managed access

IAMB core functions:[19]

- Provisioning/de-provisioning of accounts (both cloud and on-premise applications and resources)
- Authentication (multiple forms and factors)
- Directory services
- Directory synchronization (multilateral as required)
- Federated SSO
- Web SSO(e-granular access enforcement and session management; different from federated SSO)
- Authorization (both user and application/system)
- Authorization token management and provisioning
- User profile and entitlement management (both user and application/system)
- Support for policy and regulatory compliance monitoring and/or reporting
- Federated provisioning of cloud applications
- Self-service request processing such as password resets, setting up challenge questions, request for roles/resources, etc.
- Privileged user management/privileged user password management
- Policy management (including authorization management, role management, and compliance policy management)
- Role-based access controls (RBAC) where supported by the underlying system/service

Challenges:

- Insider threat
- Non-repudiation
- Least privilege/need-to-know
- Segregation of administrative (provider) vs. end user (client) interface and access
- Delegation of authorizations/entitlements
- Attacks on identity services such as DDoS
- Eavesdropping on identity service messaging (non-repudiation)
- Password management (communication, retrieval); different requirements across clients
- Resource hogging with unauthorized provisioning
- Complete removal of identity information at the end of the life cycle
- Real-time provisioning and de-provisioning of user accounts
- Lack of interoperable representation of entitlement information
- Dynamic trust propagation and development of trusted relationships among service providers
- Transparency: security measures must be available to the customers to gain their trust
- Developing a user-centric access control where user requests to service providers are bundled with their identity and entitlement information
- Interoperability with existing IT systems and existing solutions with minimum changes
- Dynamically scale up and down; scale to hundreds of millions of transactions for millions of identities and thousands of connections in a reasonable time
- Privacy preservation across multiple tenants
- Multi-jurisdictional regulatory requirements

6.12.1 PUBLIC KEY INFRASTRUCTURE-CERTIFICATE MANAGEMENT SERVICES (PKI-CMS)

PKI is a scalable security control consisting of a set of long-established techniques and standards that provides authentication, privacy, tamper detection, and nonrepudiation. PKI uses public/private keys and includes the infrastructure to manage and maintain the keys, resulting in an electronic environment that is private, confidential, and legally binding. The security industry is moving to PKI and certificates for safe internet transactions. PKI is currently the only technology that provides the required level of data integrity and protection to support electronic government.

Within a public/private cloud implementation is the need for a large-scale PKI deployment, both internal and external, as a part of identity and access management solution.

PKI-CMS core functions:

- Key distribution – how will keys be securely provided to employees, partners, devices, citizens, etc.
- Key management – who should receive keys and under what circumstances
- Key expiration – the default length of time that keys are valid, e.g., two years

[19] *Security as a Service Working Group, "Defined Categories of Service 2011." Cloud Security Alliance, 2011*

- Key rollover – re-issue of keys after a default expiration date is reached

- Key history – retaining a history of all keys issued to an entity can be important to ensure future access to items or functions protected by expired or revoked keys

- Key backup – essential for private encryption keys; not recommended for private signing keys due to the resulting risk of compromising nonrepudiation. (If someone else, for example, a system administrator, can access private signing keys, reliable authentication via the private signing key is no longer possible. However, organizations are advised to retain backups of private encryption keys to protect against technical failures or rogue encryption activity.)

6.13 SECURITY OPERATIONS MONITORING BRANCH (SOMB)

The Security Operations Monitoring Branch (SOMB) provides proactive monitoring of the technology infrastructure and data as it is used and flows into, out of, and within an organization.

Branch Services. Log management, event correlation, security/incident response, scalability, log and event storage, interactive searching and parsing of log data, and logs immutable (for legal investigations)

SOMB core functions:

- Real time log/event collection, de-duplication, normalization, aggregation, and visualization
- Log normalization
- Real-time event correlation
- Forensics support
- Compliance reporting and support
- IR support
- Email anomaly detection
- Reporting
- Flexible data retention periods and policies management, compliance policy management

Challenges:

- Standardization of log formats
- Timing lag caused by translations from native log formats
- Unwillingness of providers to share logs
- Scaling for high volumes
- Identification and visualization of key information
- Usability, segregated by client interface

6.13.1 DELIVER SITUATIONAL AWARENESS

Situational awareness will ensure that the State's enterprise is prepared to act and respond to threats to the network environment that occur hundreds of times a day and are detected by intrusion detection systems, antivirus systems, firewalls, system logs, and access logs. Many IT organizations struggle to compile the resources needed to review the data coming from all of these systems. On a network, security situational awareness is a constant ongoing health check. A zero-day threat can move through a network in seconds, wreaking havoc and putting business-critical systems at risk. The Security Operations Center (SOC) diagnoses attacks through constant monitoring of managed devices on the network and correlates the data in real-time so that operators can see what is happening as it is happening and quickly respond to the threat.

One of the SOC's most powerful functions is that it offers proactive awareness across multiple security-related systems. The SOC can consolidate all reports from the devices and tie the information together into a coherent visual representation to close windows of risk. By looking across the entire enterprise and combining this information with the data in the Network Operations Center (NOC), stealth attacks can be exposed and result in broader, more complete protection for the entire enterprise.

6.13.2 MEET BUSINESS OPERATIONS REQUIREMENTS

While each organization has its own specific security needs, there are some common top-level security information management business requirements that apply to most organizations.

6.13.3 REDUCE RISK AND DOWNTIME

For most networks and businesses, the most important requirement is to keep the network running at an acceptable risk level without downtime. In the past, it may have been possible for an organization to shut down the mail server when an e-mail virus was quickly spreading, but for most organizations, this is no longer an option. Email is a critical business function for delivering services to citizens.

The SOC must support the organization by intelligently and proactively alerting the right people at the right time about critical security events. If this risk can be mitigated before the security event begins attacking critical business systems, then the IT staff will not be forced to shut down those systems. When building the SOC, implement tools that will assist the organization to actively report security incidents in real-time using various methods for alerting, such as pagers, email, or a centralized security management console.

6.13.4 THREAT CONTROL AND PREVENTION

Organizations also must ensure that threats are either prevented or contained. This involves early notification of suspicious activity and the ability to implement a containment mechanism quickly. For example, if a firewall and network management system report the infiltration of a root kit aimed for a targeted host, the operator could be alerted to this root kit and remove it from the target host before the installation process is complete and the host has been compromised.

Organizations may not always be able to prevent threats from infiltrating a network entirely, but they can prevent their spread. Should a network system be compromised, organizations can use the SOC to quickly identify the affected hosts and lock them down from the rest of the network. Routers, switches, and VLANs could be reconfigured to limit the reach of the compromised system and prevent the spread of the threat, thus giving administrators time to remediate the risk before further damage occurs.

To feasibly contain and prevent security incidents, critical alert information must be disseminated quickly and accurately so that administrators can take action. The SOC must be able to validate and correlate alerts and information, put these events in context with the organization's network environment, and provide this critical intelligence to key staff in real-time via various alerting mechanisms such as emails, pagers, or trouble ticketing.

6.13.5 EASE ADMINISTRATIVE OVERHEAD

Organizations have implemented various threat management systems to protect them from the impact of security events. The millions of alerts generated by each individual system—such as intrusion detection systems, antivirus systems, firewalls, operating system logs, and access control systems—are overwhelming. Some organizations engage several staff members to monitor these systems for potential threats. Other organizations simply do not have the staff or budget to monitor them. Additionally, organizations are challenged to find staff with the appropriate skillsets to monitor one or more of these systems.

The SOC should be designed to involve the least amount of human overhead. The SOC provides organizations with the ability to centralize all critical security information into one single centralized console and reduce the need for multiple staff members to manage and monitor the unique devices. The goal is to empower a few administrators with the best information to enable fast, automated responses. Security information management tools that are open and interoperable make this goal easier to accomplish because the disparate data can be correlated and integrated into a single management tool.

6.13.6 PEOPLE AND RESPONSIBILITIES

State departments must agree to share trust and administrative control across departments, divisions, branches, attached agencies, and among partner organizations. For example, a state government may need to have a SOC that collects and manages information from distinct agencies such as the educational system and the police department. Leveraging the organization's security policy standards, responsibilities must be defined including who is responsible for specific tasks and assigning accountability for response and control for each business unit or agency.

As these responsibilities will be defined and communicated, the SOC tools must support these specific roles. Security information management products must provide the ability to federate trust across the departments and deliver near real-time reports based on unique roles.

6.13.7 ESCALATION PATH

A supplementary requirement to the people and responsibility need involves knowing how and when to escalate events. Consider a subsidiary company at a global corporation whose security is managed by the parent company's centralized SOC. If a fast-spreading worm is reported to the SOC and action is immediately required at the subsidiary location but the subsidiary staff is not available when the worm hits due to time zone differences, the SOC operator must know:

- Who to call to receive appropriate approval to enforce the remediation action
- Whether the nature of the threat is critical enough to implement the remediation immediately without approval

It is critical to have a SOC that is integrated within a corporate workflow chain and the Change Management systems. The security information management system should have the ability, based on the criticality of the threat and user's role, to administer the system from within the security console (restart or shut down a system), implement a remediation (e.g., push a patch through a software delivery system), or open a trouble ticket to deploy a technician to address the issue.

6.13.8 AUDIT AND COMPLIANCE SUPPORT

One of the most critical business needs that the SOC can help address is the requirement for auditing to comply with corporate, government, and industry regulations such as HIPAA, IRS 1075, and PCI-DSS. Having quick, flexible access to threat information, identity and access control data, and patch levels is critical for proving compliance. Historically, organizations rely on existing documentation or generate new documentation to prepare for an audit. The process of manually creating documentation for each audit is not only time consuming but prone to errors. SOCs are critical business tools when used for audit and compliance reporting. SOC real-time reports offer an accurate reflection of the system's current state. For example, consider an organization that has a corporate security policy for identity management that requires 30-day password aging for all accounts on all servers. The configuration settings of the servers can be reviewed, but the auditor can also use the SOC log data to search for accounts whose passwords were changed outside of the aging parameters.

6.13.9 INCIDENT RESPONSE AND RECOVERY

When systems are affected by a security event, administrators must be ready to respond as efficiently as possible to limit the damage, determine the root cause, and get the system back up and running quickly. A well-designed SOC empowers administrators to see attacks on the network and helps them leverage incident management tools to pinpoint and remediate problems.

6.13.10 MEET TECHNICAL OPERATIONS REQUIREMENTS

While the business requirements for the SOC are fairly clear and intuitive, organizations must also focus on the underlying technical components and functions needed to deliver on those business requirements.

6.13.11 SPEED OF AGGREGATION AND CORRELATION

Security devices on a network send a great deal of data and alerts. When these are aggregated into a single point for review, the sheer volume can be overwhelming. Depending on the size and complexity of the network, "a lot" can easily translate into hundreds of millions of alerts a day—far too many events for any human to monitor.

The SOC's intelligent console must support the business by sifting through these alerts quickly and prioritizing each event by its severity and threat to the business. Using security information management software, the SOC can provide information that can aid an escalation process to handle the resolution of an event, suppress repeat information, validate alerts to confirm their impact, and prioritize the most critical alerts.

6.13.12 DEVICE AND SYSTEM COVERAGE

A seemingly calm network could be teeming with problems that simply are not being reported properly. If critical devices on the network are not able to work with the security information management products, they are being overlooked and that can lead to dangerous blind spots in the network. For the SOC to deliver real value, it must support all of the security devices, servers, and applications.

Many security information management products offer integration with key threat management tools such as intrusion detection systems, firewalls, routers, operating system logs, and antivirus systems. However, additional sources such as vulnerability management systems, access management systems, business applications, physical security systems, network and system management systems, mainframe security systems, and database systems provide valuable event data that the SOC can leverage. The more data that can be gathered and correlated within the SOC, the more accurate the intelligence will be for mitigating and resolving events.

6.13.13 PROACTIVE INFRASTRUCTURE MONITORING

Zero-day threats, such as malware and viruses, can spread within minutes across the world and throughout an organization. The SOC must provide information in real-time, giving operators the data to take action immediately. At the same time, the SOC also must be able to provide automated actions and resolutions to threats such as restarting systems, initiating a trouble ticket to the help desk to initiate and implement shielding tactics, and working with a patch management system to push patches to vulnerable systems.

6.13.14 UPTIME 24/7, 365 DAYS OF THE YEAR

If a network is running 24/7/365, the SOC must also be up and running in conjunction with the network. Security information management tools help provide the high-availability support needed to meet the always-on requirement.

6.13.15 SUPPORT FOR FEDERATED AND DISTRIBUTED ENVIRONMENTS

Whether they support multiple business units, subsidiaries, or complex partner and customer frameworks, many enterprises run on a federated model. Various groups, sometimes with different business charters, manage portions of the federated network often. When it comes to managing these distributed organizational networks in a holistic manner, the SOC must support federated views and management roles. For example, a subsidiary might report all data to the central SOC, but control for remediation might not be shared with the parent organization. For the SOC to meet those parameters, security information management tools must provide flexible role-based views and accounts to accommodate these differing needs.

6.13.16 FORENSIC CAPABILITIES

Suppose an attack or vulnerability has occurred, action was taken, and the problem was remediated. Good news, right? Yes, but a thorough IT department must ask what can be learned from this incident to help prevent a similar type of attack in the future. Forensic and historical data are maps of what happened and can offer clues as to how the threat worked its way through controls and showed its path of attack. Security information management tools record the event activities report the information in the SOC, which in turn helps prioritize and visualize the data to give administrators the information needed to learn from an incident and prevent it from happening again.

6.13.17 INTELLIGENT INTEGRATION WITH SOCS AND NOCS

A SOC is an incredible business tool, but it should not work as an island. SOCs often live within or beside the NOC, and together these tools provide the statewide network and security view that businesses need for maximum efficiency. Security events can be sent to the NOC from the SOC to communicate the nature of incidents and provide additional intelligence for improved enterprise management. The NOC should have insight from the SOC so it can successfully respond to events and administer security processes and services. This bi-directional communication is necessary for organizations to respond efficiently and keep risk and damage to a minimum.

6.13.18 THE SOC IN ACTION

With the SOC gathering information, an organization can respond quickly and effectively to security events and tthreats—even internal threats—in real-time. Consider the following example:

A security administrator at a company is in a room in Colorado that is lit by the glow of numerous monitors showing physical areas of the campus. Each monitor displays data that is being reported from the distributed geographic sites of the enterprise. The administrator receives an alert on the main console, clicks a button, and then picks up a phone and places a call to a local operator in California. The administrator responds to a security alert that showed someone improperly sending proprietary information out of the company. In just a few seconds, the user's access is blocked, the local operator is dispatched to remove the user from the building, and an investigation into the incident is initiated.

Cost avoidance. Building the SOC will cost far less than not detecting, preventing, and responding to attacks.

Cost efficiencies. Many of the SOC processes or technologies can help automate functions already taking place within the organization. By accepting a new data feed and producing automated reporting, a SOC can often save the organization money by reducing manual effort.

Cost sharing. Departments within the State either do not monitor or rely on untrained individuals are tasked with the responsibilities outlined for the future SOC. Are those groups willing to outsource these responsibilities to the SOC? Having other organizations help to foot the bill can minimize the overall impact to all.

Revenue/Cost Recovery. SOC services can be offered to all State departments. There is more work in determining separation of information among departments and other business aspects, but cost recovery can be leveraged to perform security services for all state departments.

6.13.19 MULTIPLE SECURITY OPERATIONS CENTERS

The current vision for the State's new IT/IRM infrastructure is a combination of five Shared Service Centers (SSCs) across five of the Hawai`ian islands (Oahu: two; Kauai: one; Maui: one; and Hawai`i: one).

Each of these Shared Service Centers will contain a manned security operations center to provide 7/24/365 rotational, proactive monitoring of the State's infrastructure and data.

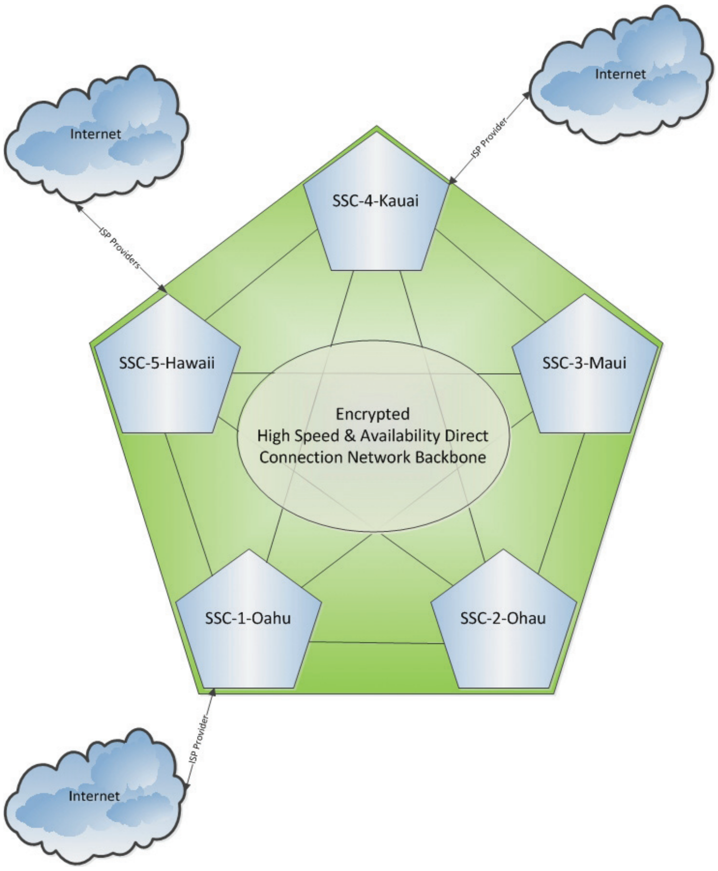


Figure 11: Shared Service Centers Vision for the State of Hawai'i

6.13.20 PRIVILEGED ACCESS MONITORING

Privileged Identity Management (PIM) is a domain within Identity and Access Management focused on the special requirements of powerful accounts within the IT infrastructure of an enterprise. It is frequently used as an Information Security and governance tool to help companies meet compliance regulations and to prevent internal data breaches by using privileged accounts.

6.14 STATE OF HAWAI`I DATA PRIVACY PROGRAM

Data Privacy and IA are often confused as the same solution. IA and CS are the tools, personnel, and monitoring, and data privacy is the result.

There are various U.S. state and international laws which govern the disclosure of personal, private, or financial information to individuals who do not have the need to know that information to properly perform duties associated with their daily work:

- Gramm-Leach-Bliley Act (GLBA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Payment Card Industry Data Security Standard (PCI DSS)
- Australia's Privacy Law
- Canada's Privacy Law
- European Union (EU) Directive on Data Protection
- Organization for Economic Cooperation and Development (OECD)

These laws sometimes conflict with the concept of open data; it is therefore imperative that any policies, procedures and standards developed as an IA and CS solution take privacy and open data initiatives into consideration.

More details on the IT/IRM Privacy compliance are available in the IT/IRM Privacy Plan.

7 ASSUMPTIONS

8 CONSTRAINTS

9 INFORMATION ASSURANCE AND CYBER SECURITY INITIATIVES

10 GUIDANCE FOR PROGRAM MANAGERS AND PROJECT LEADS

11 CONCLUDING REMARKS

7 ASSUMPTIONS

In the development of the Plan, the following assumptions were made:

- A Enterprise Risk Management philosophy and processes will be put into place.
- An IA and CS Program Management Plan will outline the details of the necessary infrastructure to implement a SecaaS model successfully.
- The CIOC and government support will prioritize resources (staff and budget) to support the recommendations of the Plan.
- An Information Assurance and Cyber Security Division will be created under the State's CIO, led by a CISO.
- Each state department (and attached agencies where applicable) will designate a Department Information Security Officer as a primary point of contact for issues, concerns, and projects related to IA and CS.

Development of the Plan and implementation of its recommendations are long-term objectives that will continue to be refined through progressive elaboration. As IT Security is a constantly evolving field, the Plan will be updated continuously to reflect changes.

The concepts and strategies identified in the Plan will remain true barring additional requirements and mandates that may affect the Plan.

Implementation of the recommendations set forth in the Plan will not completely eliminate risk; this is not possible. The intent of the Plan is to reduce risk to an acceptable level. Residual risk will be manageable and should be acceptable if the recommendations of the Plan are adopted.

8 CONTRAINTS

In the development of the Plan, the following constraints were recognized:

- Magnitude of the effort. The creation of the Plan encompasses a vast number of technologies and requirements along with associated risks and is bound by the following scope constraints:
  - – The number of risks to the environment is immense.
  - – Technology and the associated risks are constantly changing.
  - – Security requirements continue to increase.
- Resources. As with any effort, staffing and budget concerns must always be considered. The development of the Plan is bound by the following resource constraints:
  - – Decreasing budget environment
  - – Competing priorities vying for the same resources
  - – Lack of resources to remediate identified issues
  - – Increasing demands on available resources
- Implementation Challenges. Implementation of the Plan will require a great deal of effort and cooperation to achieve the level of security desired and is bound by the following implementation constraints:
  - – Legacy system concerns
  - – Policy communication and enforcement
  - – SDLC challenges; build security into the design
  - – Departmental mission impacts

9

INFORMATION ASSURANCE AND CYBER SECURITY INITIATIVES

In preparing the Plan, the IA&P-AWG team evaluated legislated requirements, prior studies and planning documents, department and organizational commitments, best practices, and the experience and knowledge of the team members to build a list of prioritized initiatives; a strategy that will help focus State's improvement efforts.

Detailed descriptions of the initiatives are in "Appendix A - Information Assurance and Cyber Security Program Strategic Investment Initiatives"

10

GUIDANCE FOR PROGRAM MANAGERS AND PROJECT LEADS

Each project initiated will adhere to the following tenants, goals, and objectives:

- Acquire and implement common enterprise security tools to maximize cost reductions with economies of scale.
- Technologies, tools, and solutions must—to the maximum degree possible—be able to be integrated in a fashion that provides automated enterprise-wide visibility into the security posture of State's information and information systems.
- Standardization decisions will be formally documented and the resulting standard, or specific product in cases where there are no standards-based solutions available, will be incorporated into the State's Enterprise Architecture Technical Reference Model (TRM).
- Consideration should be given to leveraging and integrating existing investments to the greatest extent possible to conserve available constrained budgetary resources.
- Solutions should not be conceived in a vacuum or stovepipe fashion where consideration is given towards addressing a single risk or requirement. The way other solutions collectively help to mitigate that risk while also effectively contributing towards mitigating a variety of other risks to achieve the greatest cost efficiency possible are factors.
- To achieve progress in a timely manner and to develop and maintain appropriate levels of expertise and support for each enterprise initiative, the Centers of Excellence (CoE) concept should be implemented. The CoE concept should be inclusive of the departments, divisions, and branches to participate in the incorporation of their respective requirements, vetting of all requirements, and majority consensus approach towards selecting the final solutions to include involvement in the testing and evaluation processes that result in formal standardization decisions incorporated into the TRM.

11 CONCLUDING REMARKS

Under the leadership of OIMT, the IA& P-AWG has prepared this document that recommends both a strategic and tactical approach to IT security improvements that address many of the systemic weaknesses of the State's security posture while recognizing the technical, financial, and cultural needs of State's organizational subcomponents.

In preparing the Plan, the IA&P-AWG evaluated legislated requirements, prior studies and planning documents, department and organizational commitments, industry best practices, and the experience and knowledge of team members to build a list of prioritized initiatives—a strategy—that will help to focus improvement efforts.

By adopting the recommended initiatives identified, the State's security posture can be significantly improved. Initiatives have been prioritized by the IA&P-AWG to provide the greatest immediate benefit to State. All of the recommended initiatives represent significant investments of both capital and human resources; however, the benefits derived in implementing these initiatives greatly outweigh the potential risks associated with damage to State's reputation, mission activities, and public trust.

APPENDIX A –
INFORMATION ASSURANCE AND CYBER SECURITY PROGRAM STRATEGIC INVESTMENT INITIATIVES

APPENDIX A –
INFORMATION ASSURANCE AND CYBER SECURITY PROGRAM STRATEGIC INVESTMENT INITIATIVES

A summary of each program investment is provided below that includes:

- The investment name
- Project name (where it exists in current project documents)
- The investment priority as determined by the Information Assurance Working Group; and change the last sentence on the page to read: “Risk information has been redacted for security concerns and cost estimates are not included as they are
- pending review.”
- Summary description
- Associated risk categories
- Maturity levels
- Performance periods
- Total cost remarks

For ease of distinguishing the types of investment initiatives, the tables are color-coded:

- Green—initiative is presently underway
- Purple—initiative is planned but is awaiting funding
- Blue—represents new high priorities reported to the CIOC
- Grey—represents long-term initiatives based on future IT/IRM transformation initiatives. [20]

Risk-specific details have been redacted for security concerns and cost estimates are not included as they are pending review.

Table 11 – Description of Investment Initiatives Tables

Investment Name:		1		
Priority:	2	Likelihood:	Impact:	
Current Maturity Level:			5	
Funding Source:		6		
Summary Description:		7		
Risk (if not implemented):		8		
Level of Control			Performance Period	Cost Estimate
			9	10
Estimated Total Cost:				11

Legend

1. Investment Name—title of investment used for tracking purposes

2. Priority—level of priority:

- Critical: should be implemented immediately
- High: implementation within 6–12 months
- Medium: implementation within 12-18 months
- Low: implementation within 18+ months
- As required: when Enterprise IT transformation requires new security investment
- TBD: to be determined

3. Risk Assessment: Likelihood—how likely an event would occur if without the benefit of the protection of the investment.

4. Risk Assessment: Impact—the impact an event will have on the State's infrastructure and data if the investment is not implemented

5. Current Maturity Level—the maturity level currently implemented within the state.

6. Funding Source—expected source of state funding

7. Summary Description—brief description of the investment

8. Risk—description of the risk to the states computing infrastructure and data if the investment is not implemented.

9. Level of Control: Performance Period—the expected timeframe to architect, invest, implement, and operate the level of control.

10. Level of Control: Cost Estimate—cost estimate based on data gathered from vendors or previous state implementation for the level of control described and the period of performance. These costs include the hardware, software, consultant assistance and maintenance costs over the Performance Period.

11. Estimated Total Cost—total cost estimate for the investment, over the lifetime of the *Business and IT/IRM Strategic Plan*[21] (ten-year period). Industry best practices indicate that IA and CS budgets be based on eight- to ten-percent of the annual total IT budget spending. These estimates also take into consideration the economies of scale by engaging vendors with statewide enterprise-level purchases/licensing agreements; a cost savings across all State departments can be achieved.

[21] These costs do not reflect the precise cost of the investment and are given in 2012 dollars. They do not reflect changes in inflation nor do they reflect FTE expenses to implement and operate the investment, and will be subject to change when the investment is released for a Request for Proposal.

Investment Name:	Network Data Loss Prevention (nDLP)				
Priority:	TBD	Likelihood:	Almost Certain	Impact	Catastrophic
Current Maturity Level:	Optimized				
Funding Source:	Inderpartmental Transfers - U				
Summary Description: This investment implements a system to protect Personally Identifiable Information (PII) and other sensitive data from inadvertently leaving State's network without authorization or other appropriate protections.					
Risk (if not implemented):					

Level of Control		Performance Period	Cost Estimate
Triage	Implemented software, processes, procedures and support personnel to protect Personally Identifiable Information (PII) and other sensitive data types from unauthorized use, access, disclosure, and to report on any perceived or confirmed exposure of PII.	FY 2012–13 (Dependencies: None)	
Enterprise	Implementation of data loss prevention technology to the department, attached agencies and additional areas on OneNet.	FY 2013–16	
Estimated Total Cost			

Investment Name:	IT Security Policy Assistance				
Priority:	**5**	Likelihood:	Possible	Impact	Insignificant
Current Maturity Level:	Unknown				
Funding Source:	TBD				
Summary Description: This investment will support the development and promulgation of revised policies better articulating the responsibilities of organizational components to more effectively manage their IT security programs, internal security configurations and risks.					
Risk (if not implemented):					

Level of Control	Performance Period	Cost Estimate
Assist state with development, review and implementation of a common set of security policies, guidelines, standards and procedures.	FY 2012–13 (Dependencies: None)	
Estimated Total Cost		

Investment Name:	Network Data Loss Prevention (nDLP)

Priority:	TBD	Likelihood:	TBD	Impact	TBD

Current Maturity Level:	Unknown
Funding Source:	TBD
Summary Description: This investment protects data stored on state owned mobile devices by allowing state employees traveling overseas to use devices with no state data stored on them permanently.	
Risk (if not implemented):	

Level of Control	Performance Period	Cost Estimate
Purchase mobile device pool (laptops, phones, etc.)	FY 2012–13 (Dependencies: None)	
Image Standardization for mobile devices	FY 2013–23	
Estimated Total Cost:		

Investment Name:	Data-at-Rest (DAR) Encryption				
Priority:	**5**	Likelihood:	TBD	Impact	TBD
Current Maturity Level:	Unknown				
Funding Source:	TBD				
Summary Description: This investment protects data resident on assets outside of the physical protection boundaries of State's facilities – typically resident on mobile devices that can be lost or stolen.					
Risk (if not implemented):					

Level of Control	Performance Period	Cost Estimate
DAR encryption solution implemented on all endpoint computing devices.	FY 2013–23 (Dependencies: None)	
DAR encryption solution implemented on all removable media (USB, Optical, Magnetic, etc.) containing persisting sensitive information.	FY 2014–23	
DAR encryption on server based data and databases.	(Dependencies: None) FY 2013–23	
Estimated Total Cost:		

Investment Name:	Critical Infrastructure Risk Assessment				
Priority:	5	Likelihood:	TBD	Impact	TBD
Current Maturity Level:	Unknown				
Funding Source:	TBD				

Summary Description: Hire a respected third party organization to perform security audits to determine security baseline across all state departments and identify gaps in security.

Risk (if not implemented):

Level of Control	Performance Period	Cost Estimate
Perform third party security audit	FY 2013	
Review study and develop plan of action and milestones (POA&M)	FY 2013	
Execute POA&M based on external audit gaps	FY 2013-2023	
Perform biennium external security audit	FY 2014-2023	
Estimated Total Cost:		

Investment Name:	Server Configuration Stability Monitoring				
Priority:	**5**	Likelihood:	TBD	Impact	TBD
Current Maturity Level:	Unknown				
Funding Source:	TBD				

Summary Description: This investment helps identify alterations in operating system, database, applications and security configurations that result in State's assets being more susceptible to threats.

Risk (if not implemented):

Level of Control	Performance Period	Cost Estimate
Implement within ICSD server base	FY 2013 (Dependencies: None)	
Implement statewide all servers	FY 2014-23 (Dependencies: None)	
Estimated Total Cost:		

Investment Name:	Media Disposal and Destruction				
Priority:	**5**	Likelihood:	Possible	Impact	Insignificant
Current Maturity Level:	Unknown				
Funding Source:	TBD				
Summary Description: Purchase device(s) or a service to destroy media containing state sensitive or personal data.					
Risk (if not implemented):					

Level of Control	Performance Period	Cost Estimate
Purchase media destruction equipment	FY 2013	
Enterprise level hardware retention agreements with vendors	FY 2014-23	
Estimated Total Cost:		

Investment Name:	Information Assurance and Cyber Security Professional Training				
Priority:	**5**	Likelihood:	Possible	Impact	Insignificant
Current Maturity Level:	Unknown				
Funding Source:	TBD				
Summary Description: Provide training and certification resources for IA and CS Division and DISOs.					
Risk (if not implemented):					

Level of Control	Performance Period	Cost Estimate
Initial Training & Certification Testing	FY 2013–23	
Certification Maintenance	FY 2013–23	
Estimated Total Cost:		

Investment Name:	Enterprise Domain Name Service Security (DNSSEC)				
Priority:	**5**	Likelihood:	Possible	Impact	Insignificant
Current Maturity Level:	Unknown				
Funding Source:	TBD				

Summary Description: A set of extensions to DNS that provide to DNS clients (resolvers) origin authentication of DNS data, authenticated denial of existence, and data integrity.

Risk (if not implemented):

Level of Control	Performance Period	Cost Estimate
Initial Training & Certification Testing	FY 2013–23	
Certification Maintenance	FY 2013–23	
Estimated Total Cost:		

Investment Name:	Enterprise Domain Name Service Security (DNSSEC)				
Priority:	**5**	Likelihood:	Possible	Impact	Insignificant
Current Maturity Level:	Unknown				
Funding Source:	TBD				
Summary Description: Provide means to secure, trusted communications between multiple entities across unsecure public networks using public/private cryptography key pair.					
Risk (if not implemented):					

Level of Control	Performance Period	Cost Estimate
Pilot Implementation of PKI and Certificate Authority technology within ICSD	FY 2013 (Dependencies:	
Deployment and support of PKI across all state agencies.	AD infrastructure including internal certificate authority)	
Estimated Total Cost:	FY 2014-23 (Dependencies: Enterprise wide AD deployment and I&A Management)	

Investment Name:	Automated Compliance Monitoring and Reporting				
Priority:	**5**	Likelihood:	Possible	Impact	Insignificant
Current Maturity Level:	Unknown				
Funding Source:	TBD				
Summary Description: This investment helps identify alterations in security configurations that result in State's assets being more susceptible to threats.					
Risk (if not implemented):					

Level of Control	Performance Period	Cost Estimate
Implemented continuous monitoring of security configurations on ICSD servers.	FY 2013-16 (Dependencies: Implementation of the IRM Asset Discovery and Inventory solution)	
Implemented continuous monitoring of security configurations on Department desktops and servers and department/division/bureau/office servers.	FY 2014-23 (Dependencies: Implementation of the IRM Asset Discovery and Inventory solution)	
Estimated Total Cost:		

Investment Name:	Personally Owned Remote Device OneNet Access				
Priority:	**5**	Likelihood:	Possible	Impact	Insignificant
Current Maturity Level:	Unknown				
Funding Source:	TBD				
Summary Description: Allow personally owned devices, (desktops, laptops, iPhone, iPad, Android tablets, etc.) access into state's IT Infrastructure, while still providing secure communications between the mobile device and state owned systems.					
Risk (if not implemented):					

Level of Control	Performance Period	Cost Estimate
Initial pilot project to include two-three state departments totaling no more than 500 mobile devices (one-time cost)	FY 2013	
Department-wide implementation and support (maximum 25,000 mobile devices)	FY 2014-23	
Citizen access to OneNet for access to public and private cloud services	FY 2015-23	
Estimated Total Cost:		

Investment Name:	Personal Mobile Device Management				
Priority:	**5**	Likelihood:	Possible	Impact	Insignificant
Current Maturity Level:	Unknown				
Funding Source:	TBD				

Summary Description: Remotely manage personally owned mobile devices to allow for secure communications between the device and the State’s network, systems and applications.

Risk (if not implemented):

Level of Control	Performance Period	Cost Estimate
Initial Pilot project to include 2-3 state departments totaling no more than 500 mobile devices (one-time cost)	FY 2013	
Department wide implementation and support (max 25,000 mobile devices)	FY 2014–23	
Estimated Total Cost:		

Investment Name:	Enterprise Security Operations Center(s)				
Priority:	**5**	Likelihood:	Possible	Impact	Insignificant
Current Maturity Level:	Unknown				
Funding Source:	TBD				
Summary Description: This investment supports State's ability to monitor threats presented by data loss from mission critical systems resulting from miss-configurations or unauthorized data transfers initiated by malicious actors.					
Risk (if not implemented):					

Level of Control	Performance Period	Cost Estimate
Implemented virtual capability for security event and incident monitoring, detection, reporting and response activities at Department level.	FY 2013–23 (Dependencies: None)	
Implemented integrated capability for vulnerability and security configuration compliance monitoring, threat management functions and penetration testing activities at Department level.	FY 2012–23 (Dependencies: Implementation of the IRM Asset Discovery and Inventory solution)	
Implemented integrated capability for security event and incident monitoring, detection, reporting and response activities at Department and bureau/office level.	FY 2014-23 (Dependencies: None)	
Estimated Total Cost:		

Investment Name:	Computer Security Incident Response Team (CSIRTs)

Priority:	**5**	Likelihood:	Possible	Impact	Insignificant

Current Maturity Level:	Unknown
Funding Source:	TBD

Summary Description: This investment improves computer incident detection, reporting, prioritization, response, collaboration, and resolution capabilities throughout the Department.

Risk (if not implemented):

Level of Control	Performance Period	Cost Estimate
Upgrade forensics analysis tools	FY 2013	
Forensics tools and analysis training	FY 2013-23	
Estimated Total Cost:		

Investment Name:	Enterprise Penetration Testing Capability				
Priority:	**5**	Likelihood:	Possible	Impact	Insignificant
Current Maturity Level:	Unknown				
Funding Source:	TBD				
Summary Description: This investment will define, document, and implement a core capability enabling State to assess the effectiveness of security controls, when evaluated from an attacker’s perspective, to deny the compromise of mission critical systems.					
Risk (if not implemented):					

Level of Control	Performance Period	Cost Estimate
Penetration Testing Certification (10 FTEs)	FY 2013–23	
Penetration Testing Software and Licensing	FY 2013–23	
Estimated Total Cost:		

Investment Name:	Common Standards for Protecting Privacy and Other Sensitive Data				
Priority:	**5**	Likelihood:	Possible	Impact	Insignificant
Current Maturity Level:	Unknown				
Funding Source:	TBD				

Summary Description: This investment will fund the development and promulgation of common standards for protecting privacy and other sensitive information.

Risk (if not implemented):

Level of Control	Performance Period	Cost Estimate
Implemented and promulgated common standards w/catalog of security products and services for protecting sensitive data throughout State departments, divisions, branches and offices.	FY 2013– 23	
Estimated Total Cost:		

Investment Name:	Secure Application Testing Program				
Priority:	**5**	Likelihood:	Possible	Impact	Insignificant
Current Maturity Level:	Unknown				
Funding Source:	TBD				

Summary Description: This investment develops and implements solutions and testing regimens within application lifecycle development processes to help identify vulnerabilities and weaknesses in all custom source code (Forge.mil and RDE&T model).

Risk (if not implemented):

Level of Control	Performance Period	Cost Estimate
Developed and implemented statewide an Enterprise Application Security Testing regimen with standardized processes and procedures for all custom source code, web applications and databases	FY 2014–23	
Estimated Total Cost:		

Investment Name:	Enterprise Identity and Access Management				
Priority:	**5**	Likelihood:	Possible	Impact	Insignificant
Current Maturity Level:	Unknown				
Funding Source:	TBD				
Summary Description: This investment develops and implements a strong logical authentication for network logon and in addition supports the use of those credentials for application logon, digital signatures, and encryption.					
Risk (if not implemented):					

Level of Control	Performance Period	Cost Estimate
Pilot account management process standards developed and supported by the solution; the processes and solution support the monitoring and reporting on account management activities and changes to accounts and account privileges.	FY 2013	
Account management processes and solution are defined, documented and integrated with the Enterprise Directory Services (Active Directory (AD)) and associated AD Operational Standardization; and all end-user computers are routinely monitored for unauthorized password changes to local accounts and unauthorized changes to local user groups.	FY 2014–23 (Dependency: Implementation of single state AD infrastructure)	
As the state IT/IRM resources move to a public/private cloud environment it becomes necessary to implement	FY 2015–23 (Dependency: Implementation of state public/private	
Estimated Total Cost:		

Investment Name:			Network-based Access Control (NAC)		
Priority:	**5**	Likelihood:	Possible	Impact	Insignificant
Current Maturity Level:			Unknown		
Funding Source:			TBD		
Summary Description: This investment will implement a network-based solution to prevent unauthorized systems from inappropriately accessing State’s network(s).					
Risk (if not implemented):					

Level of Control	Performance Period	Cost Estimate
Selected and deployed adequate network-based NAC solutions throughout selected bureau and office internal Local Area Networks (LANs). The network-based NAC is integrated with the host-based NAC solution within the Common End-Point Protection Platform investment.	FY 2013–16	
Deployed adequate network-based NAC solutions throughout all bureau and office internal Local Area Networks (LANs). The network-based NAC is integrated with the host-based NAC solution within the Common End-Point Protection Platform investment.	FY 2015–23	
Estimated Total Cost:		

Investment Name:	Network Security Upgrade				
Priority:	**5**	Likelihood:	Possible	Impact	Insignificant
Current Maturity Level:	Unknown				
Funding Source:	TBD				

Summary Description: This investment will implement a network-based solution to identify and automatically prevent attacks targeting State's networks and resources.

Risk (if not implemented):

Level of Control	Performance Period	Cost Estimate
Pilot implementation of new technology network perimeter security devices	FY 2013–14	
Full statewide implementation of new technology	FY 2014–16	
Estimated Total Cost:		

Investment Name:		Secure Wireless Access Solution			
Priority:	**5**	Likelihood:	Possible	Impact	Insignificant
Current Maturity Level:		Unknown			
Funding Source:		TBD			
Summary Description: This investment will support the selection, development, implementation, and migration to a standardized statewide wireless access solution(s) for both remote and local area network access.					
Risk (if not implemented):					

Level of Control	Performance Period	Cost Estimate
Selected, developed, implemented and migrated pilot organizations to a statewide wireless access solution performed incrementally in coordination with all remote access related initiatives/projects.	FY 2013–14 FY 2014–16	
Migrate all organizations to a statewide wireless access solution performed incrementally in coordination with all remote access related initiatives/projects.		
Estimated Total Cost:		

Investment Name:	Data in Motion Encryption				
Priority:	**5**	Likelihood:	Possible	Impact	Insignificant
Current Maturity Level:	Unknown				
Funding Source:	TBD				
Summary Description: This investment will support the design and implementation of secure internal network communications between mission-critical servers and locations.					
Risk (if not implemented):					

Level of Control	Performance Period	Cost Estimate
Pilot between data centers		
Implemented a common end-to-end encryption solution for the enterprise that encompasses all devices (desktops, laptops, mobile devices, workstations, servers, routers, etc.)	FY 2013–14 (Dependencies: None)	
Estimated Total Cost:		

Investment Name:	Statewide User Education, Training, and Awareness				
Priority:	**5**	Likelihood:	Possible	Impact	Insignificant
Current Maturity Level:	Unknown				
Funding Source:	TBD				
Summary Description: This investment enhances the department-wide IT security awareness and training program utilizing more frequent and targeted offerings in order to increase the state of security at State through improved education.					
Risk (if not implemented):					

Level of Control	Performance Period	Cost Estimate
Planned and designed an enhanced training program and delivered department-wide to reduce the number of security-related incidents and increase the state of security at State by institutionalizing the State IT Security Policy Handbook.	FY 2013 (Dependencies: None)	
Improved training program annually to better target reducing largest security-related incident types	FY 2013–23 (Dependencies: None)	
	FY 2013–23 None)	
Estimated Total Cost:		